GOVERNANCE IN AN EMERGING NEW WORLD

EMERGING TECHNOLOGY AND AMERICA'S NATIONAL SECURITY

Philip Breedlove, T.X. Hammes,
Margaret Kosal, Emelia Spencer Probasco,
Gary Roughead, Ralph Semmel

Convened by George P. Shultz
with James Cunningham, David Fedor, and James Timbie

A PUBLICATION OF THE HOOVER INSTITUTION

HOOVER
INSTITUTION

GOVERNANCE IN AN EMERGING NEW WORLD

Convened by George P. Shultz
with James Cunningham, David Fedor, and James Timbie

Table of Contents

WINTER SERIES, ISSUE 319

HOOVER INSTITUTION

A Letter from the Conveners

Sharp changes are afoot throughout the globe. Demographics are shifting, technology is advancing at unprecedented rates, and these changes are being felt everywhere.

How should we develop strategies to deal with this emerging new world? We can begin by understanding it.

First, there is the changing composition of the world population, which will have a profound impact on societies. Developed countries are experiencing falling fertility and increasing life expectancy. As working-age populations shrink and pensions and care costs for the elderly rise, it becomes harder for governments to afford other productive investments.

At the same time, high fertility rates in Africa and South Asia are causing both working-age and total populations to grow, but that growth outpaces economic performance. And alongside a changing climate, these parts of the world already face growing impacts from natural disasters, human and agricultural diseases, and other resource constraints.

Taken together, we are seeing a global movement of peoples, matching the transformative movement of goods and of capital in recent decades—and encouraging a populist turn in world politics.

Second is automation and artificial intelligence. In the last century, machines performed as instructed, and that "third industrial revolution" completely changed patterns of work, notably in manufacturing. But machines can now be designed to learn from experience, by trial and error. Technology will improve productivity, but workplace disruption will accelerate—felt not only by call center responders and truck drivers but also by accountants, by radiologists and lawyers, even by computer programmers.

All history displays this process of change. What is different today is the speed. In the early 20th Century, American farm workers fell from half the population to less than five percent alongside the mechanization of agriculture. Our K-12 education systems helped to navigate this disruption by making sure the next generation could grow up capable of leaving the farm and becoming productive urban workers. With the speed of artificial intelligence, it's not just the children of displaced workers but the workers themselves who will need a fresh start.

Underlying the urgency of this task is the reality that there are now over 7 million "unfilled jobs" in America. Filling them and transitioning workers displaced by advancing technology to new jobs will test both education (particularly K-12, where the United States continues to fall behind) and flexibility of workers to pursue new occupations. Clearly, community colleges and similarly nimble institutions can help.

The third trend is fundamental change in the technological means of production, which allows goods to be produced near where they will be used and may unsettle the international order. More sophisticated use of robotics alongside human colleagues, plus additive manufacturing and unexpected changes in the distribution of energy supplies, have implications for our security and our economy as well as those of many other trade-oriented nations who may face a new and unexpected form of deglobalization.

This ability to produce customized goods in smaller quantities cheaply may, for example, lead to a gradual loss of cost-of-labor advantages. Today, 68 percent of Bangladeshi women work in sewing, and 4.5 million Vietnamese work in clothing production. Localized advanced manufacturing could block this traditional route to industrialization and economic development. Robots have been around for years, but robotics on a grand scale is just getting started: China today is the world's biggest buyer of robots but has only 68 per 10,000 workers; South Korea has 631.

These advances also diffuse military power. Ubiquitous sensors, inexpensive and autonomous drones, nanoexplosives, and cheaper access to space through microsatellites all empower smaller states and even individuals, closing the gap between incumbent powers like the United States and prospective challengers. The proliferation of low-cost, high-performance weaponry enabled by advances in navigation and additive manufacturing diminishes the once-paramount powers of conventional military assets like aircraft carriers and fighter jets. This is a new global challenge, and it threatens to undermine U.S. global military dominance, unless we can harness the new technologies to serve our own purposes. As we conduct ourselves throughout the world, we need to be cognizant that our words and deeds are not revealed to be backed by empty threats. At the same time, we face the challenge of proliferation of nuclear weapons.

Finally, the information and communications revolution is making governance everywhere more difficult. An analogue is the introduction of the printing press: as the price of that technology declined by 99 percent, the volume grew exponentially. But that process took ten times longer in the 15th, 16th, and 17th centuries than we see today. Information is everywhere—some accurate, some inaccurate, such that entire categories of news or intelligence appear less trustworthy. The "population" of Facebook now exceeds the population of the largest nation state. We have ceaseless and instantaneous communication to everybody, anybody, at any time. These tools can be used to enlighten, and they can also be used to distort, intimidate, divide, and oppress.

On the one hand, autocrats increasingly are empowered by this electronic revolution, enabled to manipulate technologies to solidify their rule in ways far beyond their fondest dreams in times past. Yet individuals can now reach others with similar concerns around the earth. People can easily discover what is going on, organize around it, and take collective action.

At present, many countries seek to govern over diversity by attempting to suppress it, which exacerbates the problem by reducing trust in institutions. Elsewhere we see governments unable to lead, trapped in short-term reactions to the vocal interests that most effectively capture democratic infrastructures. Both approaches are untenable. The problem of governing over diversity has taken on new dimensions.

The good news is that the United States is remarkably well-positioned to ride this wave of change if we are careful and deliberate about it. Meanwhile, other countries will face these common challenges in their own way, shaped by their own capabilities and vulnerabilities. Many of the world's strongest nations today—our allies and otherwise—will struggle more than we will. The more we can understand other countries' situations, the stronger our foundation for constructive international engagement.

This is why we have set off on this new project on Governance in an Emerging New World. Our friend Senator Sam Nunn has said that we've got to have a balance between optimism about what we can do with technology and realism about the dark side. So we aim to understand these changes and inform strategies that both address the challenges and take advantage of the opportunities afforded by these transformations.

To do so, we are convening a series of papers and meetings examining how these technological, demographic, and societal changes are affecting the United States (our democracy, our economy, and our national security) and countries and regions around the world, including Russia, China, Latin America, Africa, and Europe.

***

The United States is engaged in strategic competition with both China and Russia, even as its technological edge erodes, and, though great-power competition may dominate the conversation, the U.S. military continues to operate in Afghanistan, the Middle East, and Africa. At the same time, we live in an age of rapid innovation, with artificial intelligence (AI), additive manufacturing, advanced computing, and other technologies enabling new military capabilities and changing how wars will be fought.

The papers in this volume address how these emerging technologies affect the strategic and operational dynamics in the two theaters of great-power competition—the Pacific and the Eurasian landmass—and with regard to non-state actors.

Former Supreme Allied Commander Europe, General Philip Breedlove (USAF, ret.), and Georgia Institute of Technology professor Margaret Kosal review Russia's traditional approach to innovation and consider how major emerging technologies, including advanced manufacturing and materials, might be employed by Russia, the United States, and its NATO allies.

Emerging technologies, argues the National Defense University's Colonel T.X. Hammes (USMC, ret.), give non-state actors military capabilities traditionally only available to major powers, thereby shifting the balance of power in their favor. The United States must reconsider its old assumptions and carefully redefine its strategy for dealing with non-state adversaries armed with these new capabilities.

Finally, we look to the Pacific with our Hoover Institution colleague Admiral Gary Roughead (USN, ret.) along with Emelia Spencer Probasco and Ralph Semmel from the Johns Hopkins University Applied Physics Laboratory, where we see that information dominance will be central to the U.S.-China competition. New technologies, from AI and autonomous systems to space capabilities, are changing the nature of conflict, requiring a rapid evolution of both military technology and operational concepts.

We look forward to the discussion of this important issue, and we thank our colleagues at the Hoover Institution who have supported this project, particularly Shana Farley and Rachel Moltz for their work on this volume.

George P. Shultz
Thomas W. and Susan B. Ford Distinguished Fellow

James Timbie
Annenberg Distinguished Visiting Fellow

Emerging Technologies and National Security: Russia, NATO, & the European Theater

By Philip Breedlove and Margaret E. Kosal, Georgia Institute of Technology

Introduction[1]

Emerging innovations within today's most cutting-edge science and technology (S&T) areas are cited as carrying the potential to revolutionize governmental structures, economies, and life as we know it; others have argued that such technologies will yield doomsday scenarios and that military applications of such technologies have even greater potential than nuclear weapons to radically change the balance of power.[2] Those S&T areas include artificial intelligence and robotics; hypersonics; additive manufacturing (aka 3D printing); meta-materials (nanotechnological materials that enable stealth/invisibility across multiple parts of the spectrum); directed energy weapons; energy generation, storage, and transmissions; the cognitive neurotechnologies (for brain-computer interface); biotechnology, including systems biology; and the intersection of each with information and communications technologies (ICTs).

When NATO conducted its first strategic review since the dissolution of the Soviet Union, almost a decade ago, it observed:

> Less predictable is the possibility that research breakthroughs will transform the technological battlefield. Allies and partners should be alert for potentially disruptive developments in such **dynamic areas as information and communications technology, cognitive and biological sciences, robotics, and nanotechnology** [emphasis added]…The most destructive periods of history tend to be those when the means of aggression have gained the upper hand in the art of waging war.[3]

That passage conceptually highlights the uncertainty, complexity, and issues of interdependence that exist in trying to understand the interactions between emerging technologies and international security. Predicting how these new innovations and breakthroughs in scientific understanding may be used is a challenge. Looking to history is one valuable past insight. One must be careful, however, to not be purely technologically deterministic. That is to not assume that because something is possible, or because something potentially may come about, that it is inevitable. History shows us that human ingenuity and use is more often a function of political decisions, regional security threats, and other factors of social, political, historical, economic, and cultural origin.

While the suggestion that such emerging technologies will enable a new class of weapons that will alter the geopolitical landscape—*including questions of challenging or changing strategic stability*—remains to be realized, a number of unresolved security puzzles underlying the emergence of these new technology areas have implications for U.S. national security, defense policy, foreign policy, governance, and arms control regimes. The extent to which these emerging technologies may exacerbate or mitigate the global security and governance challenges that Russia currently poses and will pose in the future to the United States and NATO allies will be examined.

As the United States looks to the future—whether dominated by extremist groups co-opting advanced weapons in the world of globalized non-state actors or states engaged in persistent regional conflicts in areas of strategic interest—new adversaries and new science and technology will emerge. Choices made today that affect science and technology will impact how ably the United States can and will respond. The changing strategic environment in which security operations are planned and conducted impacts S&T policy choices made today and affects how S&T may play a beneficial or deleterious role in the future. Some game-changing technologies have received global attention, while others may be less well known; these new technologies and discoveries may significantly alter military capabilities and may generate new threats against military and civilian sectors.

Future trend analysis is a tricky task. Colin Gray said, "Trend spotting is easy. It is the guessing as to the probable meaning and especially the consequences of trends that is the real challenge."[4] How, when, where, and in what form the shifting nature of technological progress may bring enhanced or entirely new capabilities, many of which are no longer the exclusive domain of the United States, is contested and requires better analytical tools to enable assessment. Contemporary analyses of these emerging technologies often expose the tenuous links or disconnections among the scientific and technical realities and mainstream scholarship on national and international security, especially with regard to the potential to have impact on strategy and policy. The research underway is advancing the strategic understanding of these game-changing technologies and the development of meaningful and testable metrics and models to help reduce that surprise.

This paper, prepared for the Hoover Institution's *Governance in an Emerging New World* project, seeks to assess the implications of new and emerging technologies for national security, with specific emphasis on Russia, NATO, and the European Theater. The paper begins with an introduction and overview of what the authors consider the broader importance of the role of technology as a factor (not *the* factor) of importance in national security and military affairs. Next, the paper places itself in the context of previous work on disruptive, emerging, and advanced technologies and conflict, including the idea of revolutions in military affairs. That is followed by a discussion of Russian technology development, including leveraging historical experience from the Cold War and institutional politics. This is critically important in order to avoid the trap of technological determinism, i.e., assuming that a state will pursue something on technological grounds only. An analysis of the national security implications of select emerging technologies—additive manufacturing (aka 3D printing), machine learning and artificial intelligence, advanced stealth via metamaterials, hypersonics, and directed energy weapons—follows. A brief discussion of trends in U.S. entrepreneurship follows. The paper closes with an analysis and conclusions pertinent to the charge from the *Governance in an Emerging New World* project's organizers, to assess implications of emerging technology for U.S. national security with emphasis on NATO and Russia.

Broader National Security Environment

In order to understand the changing paradigms for national security in the 21st Century, it is crucial that policymakers have an awareness of the factors driving new and emerging capabilities; possess the ability to analyze the changing nature of technological progress and assess potential impacts on the nature of conflict; and understand the relationships among cutting-edge science, advanced technology, other trends, and national security.

Dominance in both conventional and sophisticated military operations has been enabled in the United States by a technological advantage in precision, speed, stealth, and tactical intelligence, surveillance, and reconnaissance as compared to adversaries. Equally innovative and more revolutionary capabilities will be required in order to ensure dominance and security in the 21st Century—when adversaries span from peer competitor nation-states to disperse insurgencies and lone-wolf non-state actors.

In 2006, the Defense Science Board (DSB) was charged with looking back to the Cold War and the technologies and concurrent capabilities—precision, speed, stealth, and tactical ISR —that gave the U.S. a technological advantage over adversaries and identifying equivalent technological capabilities for the 21st Century.[5] They concluded that technological superiority is a strategic differentiator for the United States. As a result of evolving conditions, the U.S. cannot assume that it will stay ahead of its adversaries by simply spending more on research, development, and procurement. The DSB report also concluded that the global environment in which the DoD operates had fundamentally changed, and that the DoD no longer leads most technology development. Globalization of technology has leveled the playing field internationally, and the U.S. faces more complex security challenges than at any time in its past. Additionally, adversaries are increasing their ability to adopt and adapt technology more rapidly than the DoD. The changing global environment requires the DoD to carefully evaluate, shape its programs in response, and be willing to take risks.

Scientific and technological innovations have been the backbone of American economic, military, and political power since the advent of the industrial revolution. Federal support for research and development was invigorated by the arguments and evidence put forth in Vannevar Bush's now-famous report to the President in July 1945.[6] At that time, the revolutionary power and security implications of research-driven development of the atomic bomb was palpable to American policymakers, the civilian leadership in the Department of War, and the armed forces. Advances in federally-sponsored technology made the United States and its armed forces the most technologically advanced in the world.

What are the roles and significance of emerging technologies and how should the national security community respond to the promise and perils of emerging technologies? How will these nascent scientific and technological developments impact local, regional, and international security, stability, and cooperation? What are the most likely sources of technological surprise with the largest threat capacity, and how can the national security community better identify them sooner? Emerging technologies present regional security challenges and may exacerbate (or mitigate) the geo-political, military, energy, and economic challenges in the future to a state or region and the potential impacts on U.S. interests and national security. Deep strategic and practical understanding of the significance of emerging technology and its diffusion as well as extending thinking concerning how science, technology, and inter- and intra-national social relations interact to shape and facilitate management of the changing global security landscape is a pressing need for the 21st Century.

The authors readily acknowledge that there are additional factors beyond technology that play a role and may drive a changing, new strategic environment. These include, but are not limited to, demographics—smaller populations in some states, youth bulges, and increasingly aging populations in other states. Outside of Russia, much of the discussion revolves around megacities and dense urban conflict, which is about people and environments not just structures.

The balance across the acquisitions "iron triangle" of survivability, mobility, and lethality (or firepower) will very soon reach the end of an 'era' of physical mass providing protection, even for ground troops. With a near-peer competitor and other operating scenarios, it is likely to be those capabilities that shift the approach to survivability from protection via mass (which is limiting) to capabilities for active defense, capabilities such as meta materials, which can make objects invisible, or ideas like the use of "swarms" by adversaries. In terms of lethality, directed energy weapons are needed; we have to get away from solely relying on traditional explosives and heavy projectiles. New ways to generate, store, and convert power are needed, including at the individual level, such as through harvesting otherwise wasted energy of bootsteps striking the ground or other movements.[7] Information and communications technologies are emerged—not emerging technologies. When the individual is directly connected to the internet or other enhancements are possible, what does that mean for the laws of war? People are likely to learn more quickly by computers hooked into the mind. Do we want to go to that? We may be forced to go to that. The use of augmented reality and man-machine interface portends questions of how such cutting-edge capabilities will affect balance of power and conflict. The authors do not claim to project how an adversary will fight—no one's crystal ball has that level of fidelity—but looking to such emerging technologies offers scenarios to capabilities in which mass is relied upon to provide protection so it doesn't limit mobility.

Communication of those new discoveries is occurring faster than ever, meaning that the unique ownership of a piece of new technology is no longer a sufficient position, if not impossible. The information revolution and globalization themselves have been major drivers. It is widely regarded that recognition of the potential applications of a technology and a sense of purpose in exploiting it are far more important than simply having access to it today. Technological surprise has and will continue to take many forms. A plethora of new technologies are under development for peaceful means but may have unintended security consequences and will certainly require innovative countermeasures. For example, tremendous developments in biotechnology have occurred since the advent of recombinant DNA and tissue culture-based processes in the 1970s. If the potential for biotechnology to affect fundamental security and warfighting doctrines had been more clearly recognized twenty years ago, the situation today could be very different. Defense against biological weapons—from both states and non-state actors—currently presents a threat that is difficult to predict and for which traditional solutions are increasingly less effective and offers an area for strategic foresight to be valuable.

The dual use conundrum applies to all modern technologies. Because of the other characteristics of the changing strategic environment, it is of greater concern. Historically, dual use previously referred to technologies that could be meaningfully used by both the civilian and military sectors. In light of an ever-changing security environment in which the potential for technologies to be misused by both state and non-state actors has become increasingly prevalent, however, a new conceptualization of dual use, in which the same technologies can be used legitimately for human betterment and misused for nefarious purposes, such as terrorism, has emerged. The National Institutes of Health's Office of Science Policy has promulgated a similar understanding of dual use in its discussions and policies on biosecurity. In keeping with these understandings, this work adopts a similar definition of dual use as research "conducted for legitimate purposes that generates knowledge, information, technologies, and/or products that could be utilized for both benevolent and harmful purposes,"[8] i.e., research that can have beneficial impacts as well as unintended deleterious consequences.

Technology and War—The Scholarly Context

Within international security, there is a rich literature exploring the intersection of science, technology, and understanding the outcomes of armed conflict.[9] Similarly, for scholars of science and technology studies, the intersection of new technology and weapons application has a rich literature.[10] For strategists and scholars of revolution in military affairs (RMA)[11] and of fourth and fifth generation warfare (4GW & 5GW),[12] the nexus between technology and military affairs is not just speculation but a reality that bears directly on the propensity for conflict and outcomes of war, as well as the efficacy of security cooperation and coercive statecraft. It is a critical variable in international security: military outcomes and technological advances are intricately tied.

The offset strategy is a central concept applied to national security involving technological capabilities. Offset strategies have used technical innovation to counter the strength of adversaries and deter them. Three offset strategies since WWII are commonly cited. The first offset strategy used a nuclear-based deterrence strategy to offset Soviet land forces, proximity to Europe, and conventional superiority in Europe. In order to counter and deter the Soviet adversary, the United States relied on massive retaliation and use of nuclear weapons. The first offset strategy was a success. The second offset began in the 1970s. As the Soviets developed their nuclear arsenal and delivery systems, a new strategy was needed to counter and deter the Warsaw Pact's numerically superior conventional forces and address Soviet advances in strategic nuclear capabilities in the late stages of the Cold War. The second offset strategy invested in the development of stealth aircraft, precision guided munitions, and space-based reconnaissance and navigation capabilities. Second offset capabilities and U.S. military superiority were demonstrated during the First Gulf War.

The disruptive technology of the second offset has proliferated widely and adversaries (specifically, near-peers) have narrowed the technology gap. In 2014, the call for a third offset was put forward.[13] The DoD sought a strategy-based, technology-oriented approach to maintaining and renewing U.S. military advantage.[14] Technologically, the third offset focuses on autonomous learning systems, human-machine collaborative decision-making, assisted human operations, advanced manned-unmanned system operations, and network-enabled autonomous weapons and high-speed projectiles.[15] In addition to technology, the third offset emphasizes operational and organizational innovation, and innovative military and civilian talent management.

To be disruptive, technologies do need not be radical or novel from an engineering or technical perspective.[16] In fact, another class of disruptive technology is important to acknowledge: Innovative use of existing technology. Using a combination of existing technologies in ways that are novel can result in a capability that is disruptive.

Disruptive technology is distinctive because it upsets the established way of doing things. Disruptive technology causes shifts that change the world. Novel technologies are one of the principal means of surprising advisaries or competitors and of disrupting established ways of doing things. It is, however, important to recognize that not all innovative, novel, new, or emerging technologies or innovative uses of technology are disruptive. Some new technologies and capabilities stay in the laboratory, many start-ups fail when taking the technology to market, and plenty of new and innovative technologies or uses of technology never disseminate.

When examining a potentially disruptive technology, the scale of dissemination is a useful factor in determining whether a technology is truly disruptive. Adoption is one critical measure of a technology becoming a disruptive technology. If a technology is not adopted, then it cannot be employed. Understanding what technologies are adopted and then disseminated widely is key to determining which technologies will earn disruptive status. Based on the discussion and sources above, for the purposes of this paper, disruptive technology is defined as: an innovative technology or use of technology that triggers unexpected effects and also upsets the established way of doing things.

Disruptive technologies are distinct from "normal" technology because of the scale of their impact. As discussed above, not all scholars agree on the criteria for disruptive technology. What is important to garner from this definition is that disruptive technology has a wide and profound impact on the established ways of doing things. By its very nature, global stability can be challenged by technology that disrupts the established governance system.

New and unpredicted technologies are emerging at an unprecedented pace around the world. Communication of those new discoveries is occurring faster than ever, meaning that the unique ownership of a new technology is no longer a sufficient position, if not impossible. In today's world, recognition of the potential applications of a technology and a sense of purpose in exploiting it are far more important than simply having access to it.[17] Advanced technology is no longer the domain of the few. In the 21st Century, both nation-states and non-state actors will have access to new and potentially devastating dual-use technology.

Anticipating the types of threats that may emerge as science and technology advance, the potential consequences of those threats, the probability that new and more disperse types of enemies will obtain or pursue them, and how they will impact the future of armed conflict is necessary in preparing for the future security of the nation. The potential synergies among the emerging technologies not only suggest tremendous potential for advancement in technology for military applications but also raise new concerns.

With Russia, one needs to consider not only advances in high technology for traditional military applications but also innovations and uses below the level of declared war, i.e., what is referred to as hybrid warfare, the grey zone, non-linear war, or war below the line (of the Gerasimov "doctrine"). These terms have been taken to mean literally the use of subversion, information warfare, and covert activities to prepare the battlefield before intervention, or what George Kennan called political war: "the employment of all the means at a nation's command, short of war, to achieve its national objectives,"[18] seeking to undermine U.S. influence abroad and in Europe specifically and to weaken the post-WWII international order. Leveraging all aspects of national power, political warfare spans military, diplomatic, information, and economic arenas and includes both covert and overt activities.

Additionally, while the calculus for use in a traditional state-on-state military conflict may not have changed substantially,[19] Russia and its allies are using chemical agents in non-traditional ways. Chemical weapons, which once seemed to be nearing status as an artifact of history in the first decade of the 21st Century, have re-emerged as weapons for targeted assassinations by states like Russia and the DPRK and for use against insurgents and civilians as part of Syria's civil wars. The long-standing chemical weapons taboo has been shattered, repeatedly.

Understanding Russian approaches to technology development would not be complete without acknowledging the role that dezinformatsiya, disinformation, and maskirovka, military deception, play in interactions with external actors. Soviet training manuals trace the 'science' of disinformation back to 1787, when mock villages were built in Ukraine to give an impression of prosperity as Catherine the Great, Empress of Russia, passed through the countryside.[20] Traveling throughout Russia in the 1700s, the French Marquis de Custine noted in his journals, "Russian despotism not only counts ideas and sentiments for nothing but remakes facts; it wages war on evidence and triumphs in the battle."[21] Two centuries later, the Soviets instituted deception as a national policy, distorting perceptions of their society and laying the foundation for modern disinformation campaigns in military conflict. Personal leadership, geopolitics, operational context, and evolution of technology all influence the conduct of disinformation campaigns.

Overview of Russian Technology Development

There are aspects of Russian strategic culture that have remained consistent from the early origins of the Russian state, throughout the Tsarist and Soviet periods.[22] In the words of one scholar who highlights the militarized nature of Russia's culture, "[t]he continuity of Russian strategic culture through all of these changes, strategic in their character, is truly striking."[23] Russian and Soviet military strategic cultures have shown remarkable tenacity in the midst of societal upheaval, political restructuring, and changes in capabilities.[24] When examining the literature about Russian innovation, there is significant overlap between scholarship produced during the Cold War and that of the contemporary literature. This is a consequence both of the remnants of Soviet government and culture that color, if not dominate, the Russian Federation today and the sheer volume of literature on the subject produced by military and academic scholars during the decades-long arms race. This section will attempt to outline the variety of approaches to this topic that have helped shape both Western and Russian scholars' understanding of this phenomena. It will begin with a brief overview of scholarship about the Soviet process of innovation and then summarize the work of contemporary scholars attempting to make sense of the current Russian system of innovation.

Scholarship regarding military and technological innovation within the Soviet Union provides an insight into the evolution of Western opinions toward Russia. Early writers center their theories about Soviet innovation squarely in the predominant theoretical model of the time: Realism. These authors tend to approach their subject with a particular conceit; they believe that the arms race between the United States and Soviet Union stemmed from a sense of competition between the two states and wrote dozens of articles illustrating how this model shaped the politics of the Cold War and how it should shape relations between the two countries in the future.

Much of the early literature summarizing Russian technological innovation is grounded in the decades-long arms race of the Cold War. Although the specific details of the cases addressed in these studies may appear superficially outdated, many of these frameworks are useful to the discussion of the current state of innovation in Russia because they provide benchmarks by which one can compare aspects of contemporary Soviet efforts to innovate. In this model, Soviet and American leaders were locked in an endless cycle of arms balancing 'one-upmanship' that the authors refer to as the "action-reaction" dynamic of innovation between the two states.[25]

Former Secretary of Defense Robert McNamara utilizes a similar frame of reference in a much later article as he attempts to provide guidance on how the United States should address and improve relations with Russia and China in a post-Cold War world. The United States is the greatest power in the international system, and, as such, is the "winner" of the Cold War. However, he credits Russia's desire to modernize both its military and its economy to a variety of policies and actions that the United States has adopted in the wake of the collapse of the Soviet Union. Three "betrayals" that occurred during the 1990s are especially important. The first, America's expansion of NATO in the late 1990s, violated what the Russians understood to be America's promise not to expand the organization eastward in the wake of the Cold War.[26] Not only did the passage of the bill break this promise, but it also provided the Russian government evidence that the United States was attempting to contain them and their influence in Europe despite the Cold War being long since over. Secondly, the Russians understood the United "Founding Act" of May 1997 as an opportunity to obtain a commitment from the United States and NATO that would "limit the expansion of NATO's military capabilities[…]; disavow any intention to use force against any state except in self-defense or unless authorized by the U.N. Security Council; and grant Russia a role in NATO's political decision making." Although Russia secured the first two objectives, its failure to accomplish the third led directly to what McNamara considers the third betrayal:

the bombing campaign against Belgrade. While the West conceived of this bombing as a means of forcing the Serbs to stop the ethnic cleansing of Albanians in Kosovo, Russia saw the bombing as a flagrant violation of the Founding Act. The violation, in combination with the ineffectiveness of the Serbs military equipment against NATO forces drove the Russian government to improve its conventional weapons so that the country could defend itself against potential NATO attacks with something other than nuclear weapons. Such theories provide a plausible explanation for the Russian government's mistrust of the United States and its intense focus on improving its conventional weapons systems. Like the Soviet Union, the Russian Federation's process of innovation is predicated upon its desire to keep pace with the United States.

Beginning in the 1970s, however, a different program of research began to emerge on this subject. Rather than focusing solely on the balance of military capabilities of individual countries, scholars sought to understand the connection between a state's military innovation capabilities and various social-political-economic-institutional factors, as well as the long-term influence of history, known as strategic culture.[27] The literature of this time can be generally scoped into six avenues: civil-military, intra-service, international, cultural, top-down, and bottom-up.[28]

The differences between American and Soviet military innovation can be attributed to a series of cultural variables rather than strictly to military competition. Notable scholar Dima Adamsky attributes the pattern of Soviet innovation following American innovation to the structure of the Soviet military itself.[29] In his view, the highly centralized, administrative structure of the military meant that any decision to begin development of a new weapon or weapons system came from the General Secretary of the Communist Party. As such, Soviet military innovation was entirely dependent on the leaders' perception of American military strategy. Specifically, he posits that "The relationship between technology and military innovation is not deterministic, but rather socially constructed; national military tradition and professional cultures interact with technology, affecting the course and outcome of military change."[30] According to this theory, the Soviet Union constitutes a "high-context" society that draws frequently on a sense of shared history and tradition. Time is also perceived in a very non-linear manner; individuals' frequent reliance on past experience creates a culture where the present is colored heavily by the past. There is a strong sense that "everything will happen in its time" and that "everything is connected to everything else."[31] Adamsky claims that this understanding of time leads to workplace behavior that is less-than-ideal for innovation; specifically, he claims that cyclical behavior is common in the workplace, meaning that individuals frequently change from one task to another and, though they may understand a great deal, do not concentrate on any one task for long periods of time.

Another scholar, Cornell University's Matthew Evangelista, also attributes Soviet innovation to a set of particular cultural ideals but focuses on how these ideals were codified in the larger structure of the Soviet military. He is particularly interested in the intersection of the Soviet military's tradition of suffering as a precursor to strength and forbearance and the prevailing political notion of Communism. In his book *Innovation and the Arms Race: How the United States and Soviet Union Develop New Military Technologies*, Evangelista argues that Russia was a "late, late industrializer" that instituted a "costly campaign of forced-draft industrialization," inadvertently creating a highly centralized government and a very weak society.[32] He goes on to explore the State's military and history of innovation, comparing it with the United States in regards to centralization, complexity, formalization, interconnectedness, and organizational slack, five structural characteristics "that appear to affect organizational innovativeness."[33] After comparing the two states in these areas, the United States' R&D apparatus makes it inherently more innovative because the Soviet Union's "highly centralized, hierarchal," system, "characterized by excessive secrecy and compartmentalization," hinders both its ability to innovate and its ability to implement those innovations.[34] The centralization of the Soviet system, which was carried over to the Russian Federation, prevents the technologists who are willing and able to innovate from doing so until large-scale structural changes can take place in the leadership's vision for the future.

Adam Stulberg and Michael Salomone focus on another critical, often overlooked aspect of transformation: changing an organization's culture, or more specifically, ensuring that internal mechanisms manage and sustain change, writ large, once introduced.[35] Looking at Russian nanotechnology development, Stulberg highlights the uncertainty associated with that emerging technology area, and he notes the structural factors that hinder revolutionary technology development.[36]

In Soviet military writings that were classified by the Soviet Union, as early as 1962, military thought leaders discussed a coming revolution in military affairs for which the Soviet Union's military would be required to change its theory and practice in military operations.[37] In the late 1960s, Soviet military writers emphasized the importance of detecting a surprise nuclear attack given the development of precision-guided weapons.[38] In 1983, the Soviet Union was convinced that the United States and NATO planned a pre-emptive nuclear strike under the guise of NATO Able Archer exercises according to declassified documents, including a transcript of a speech by Andropov, head of the KGB at the time, to the Soviet Communist Party

Congress.[39] A persistent world view that Russia and its territories, under the Tsars and later as the central Soviet apparatus, is indefensible and subject to surprise attack by "imperial powers" pervades the Soviet military and civilian leadership's thinking during this time, driven in part by what the Soviet military community deemed a "Military Technical Revolution" with the introduction of precision-guided weapons, and later named the Revolution in Military Affairs (RMA).

Post-Cold War military writings about the RMA include aspects of information technology as well as precision-guided weapon systems and their potential impact on war. A 1997 analysis of these publications in Russian military journals revealed that there is some disagreement as to how future war will be waged, but a common theme seems to be an emphasis on the impact of technology on Command and Control as well as discussion of indirect methods of war.[40] Though General Gerasimov's 2010 comments on indirect methods of war are sometimes discussed by national security scholars as the origin of Russia's current military philosophy, it should be noted that retired military officers were debating as early as 1994 the importance of indirect methods of warfare and the role of information operations as integral to a Russian approach to modern war.[41]

We are able to account for the Soviet military's inability to capitalize on its understanding of the coming Revolution in Military Affairs in that the leadership predicted but could not implement. Scholarship about contemporary Russian innovation draws heavily on existing commentary on innovation in the Soviet Union. Prominent authors argue that many of the current problems plaguing the Russian government's efforts to streamline innovation lie in its desire to both restructure and preserve aspects of the Soviet government that have endured in the wake of the Soviet Union's dissolution, an artifact of the hybrid nature of the current government structure.

Others assert that the current state of the Russian government is influenced by the country's conflicting desires to both retain the remnants of the Soviet Union that remain in the government structure and reform the government entirely.[42] Such analysis of the Russian government's current attempts to spur innovation in its economy step into the gap left by theories of Soviet innovation by explaining the extent to which the Russian Federation's current policies are predicated on its past. Radosevic argues that Russia is currently in the midst of an innovation crisis due to its desire to both restructure and preserve what remains of the Soviet innovation infrastructure. While understandable, there are two major problems with continuing to employ this model in the future. First, because the Soviet Union understood R&D as the main generator of technological innovation, other important aspects of the innovation process such as "the role of users, engineers, and others not directly involved with R&D" were never considered.[43] As such, these avenues continue to be neglected by the current government. Secondly, the Soviet government perceived technology as a commodity that, once developed, "could be transferred into or introduced into production without need for continuous adaptations and improvements." The latter is problematic not only for continuing to foster innovation within the scientific community, but also for the quality of Russian products meant to compete on the international stage. As such, many scholars find it impossible to begin to understand the Russian government of today without accounting for its past.

Attempts have been made to synthesize many of the Russian government's current innovation efforts by examining recent legislation attempting to generate ties between the primary engine of innovation in both the Soviet Union and the Russian Federation—the independent research institute—and universities.[44] The difficulty of enacting such change, which seems utterly logical to a Western audience, takes on an entirely new meaning if the role of the university in the Soviet Union is understood. A.I. Terekhov has also written a great deal on the evolution of scientific research programs within the Russian Federation.[45] Citing a number of factors already articulate, he also highlights what he calls "the crisis of national research personnel" due to negative demographic trends.

Russia's unique strategic situation results in the deeply rooted assumption that Russia requires a unique approach to security and conflict. According to Paul Nitze, asymmetries favorable to the Soviet Union in civil defense and industrial dispersion impacted their calculations regarding various warfighting strategies.[46] Russia's unique political-military landscape and economic-technological base continue to inform its strategy. This concept is exemplified in the development of the Russian concept of hybrid warfare as, "a modern example of strategic uniqueness in Russia's culture producing an asymmetric approach to war that diverges from Western concepts and practice."[47] By basing an approach on Russian strengths and the weaknesses of adversaries, it becomes inevitably different from that of their neighbors and adversaries. Russian strategists actively acknowledge these differences and deem them necessary for strategic success. Regardless of Russian intentions, the difference in assumptions and values in Russian strategic culture and those shaping strategic culture in the West will impact European security.

Although the authors and subjects mentioned above are diverse, each fills an important role within the literature at large. The Russian Federation is notoriously resistant to sharing information about the manner in which their government functions, which gives these authors' work an important weight when attempting to ascertain where the Russian Federation is in implementing its plans for the future. It is impossible to synthesize such a large and varied literature without omitting important voices on the subject; the authors and reports included above, however, represent the most widely cited papers in this field. As such, the views and arguments can be understood to represent a far larger body of work in each area.

Legislation, Policy, and Organizational Structures

Because the Russian R&D apparatus remains highly centralized, the majority of prominent organizations encouraging innovation are tied to the government. The Russian government's current approach to innovation in many ways mirrors the process that took place in the Soviet Union. Just as the Soviet government funded the bulk of R&D activities through state-owned branch research institutes, Russia's current structure boasts a large network of research institutes that are largely separate from both industrial firms and the university system.[48] These institutes, known collectively as the Russian Academy of Sciences (RAS), are more than thirty component organizations that publish independently and compete for state funding as individual entities. Among the most prolific of these institutes are: The Nesmeyanov Institute of Organoelement Compounds RAS, The FSI Technical Institute for Superhard and Novel Carbon Materials, Lomonosov Moscow State University (MSU), The Institute of Microelectronics Technology and High Purity Materials (IMT) RAS, and The Landau Institute for Theoretic Physics (ITP) RAS.[49] While similar institutions can be found throughout Western Europe and the United States, the model under which Russia's current innovation initiatives continue to cling is reminiscent of what existed under the Soviet Union. One hallmark of this model of development is the large gap that exists between the RAS research institutes and the university system.[50] As in the past, many universities remain responsible for educating students but conduct very little research. As such, Russia's research institutes lack the ability to attract young minds to their research. This is problematic both because of the increasing need for competent young scientists to carry on the research of the aging scientific community and because it may prevent many of the mechanisms by which the Russian government hopes to stimulate economic growth in the scientific community from being sufficiently successful in the future.

Legislation enacted in the last decade provides evidence that some of the traditional government structures responsible for inciting innovation are beginning to be reformed, however. While still in the early stages, many of the Russian government's programs in this area seem to aim to increase growth in the private sector rather in particular. In 2005, the government passed a law incentivizing the creation of special economic zones (SEZs) to attract investment in manufacturing and "high-technology" development.[51] Incentives such as tax and customs breaks, financial guarantees, and "special credit conditions" are included in the bill for up to ten years as long as member corporations are willing to register with the government. After ten years, government incentives are lessened considerably in an attempt to ensure that startup corporations in these regions are able to function as competitive entities. The law also requires all member corporations—including multinational corporations (MNCs)—to submit to the same vetting process for residency in the SEZ and to apply for any grants made available to residents of the city. MNCs could thus be denied participation in the SEZ if their proposed projects fall outside the goals of the technopark. Although turning established corporations away seems counterintuitive, the government's oversight in this manner is one of a series of legislative necessities associated with successful SEZ.

A second component of successful SEZs was incorporated into Russian law in January 2008 when the Russian government passed the Federal Law On Science, which allows research institutes and universities to share material resources, workforce, and facilities free of charge.[52] More importantly, the law allows universities and research institutes to form joint entities.

Law 217 seeks to encourage further collaboration among universities and private industry by "encourag[ing] companies to establish partnerships with universities and get engaged in joint R&D activities and technological innovations.[53] Federal Government Directives 218-220 provide the legal authority for the collaborations to begin.

These collaborations allow universities and research institutes to become more responsive to the needs of the market, one of the biggest problems that the Soviet innovation system faced prior to its dissolution. For many years, the government's research demands usurped the market's, meaning that innovation occurred outside of the realm of citizens or investors' wants or needs. Increased collaboration between the research institutes and universities is meant to address this problem by providing the research institutes an arm that targets consumer needs specifically. Such changes are essential if Russia is to stimulate innovation in its economy and keep pace with other nations who it views as its largest competitors.

Even as these programs seek to stimulate the economy, however, the obvious continued reliance on the government as the driver of innovation harkens back to the Soviet apparatus. While some steps are being made to loosen the government's control over many of the major institutions within the innovation apparatus, reality of the country's current economic state and population poses its own problems. While the Soviet Union was long regarded as one of the leading countries in the number of highly educated individuals within its population—Russia still retains one of the best-educated populations in the world according to OECD data—strict divisions between the government, military, universities, and research institutes have led to a smaller number of science and engineering graduates over the years.[54] The decreasing number of science and engineering graduates means that research institutes are hiring increasingly fewer staff with masters or doctoral degrees. As such, the quality of the work being released by these entities is falling, but it also calls into question their future sustainability. Both of these considerations could prove disastrous for the SEZs slated for development in the country, as the reputation of the corporations participating in these startups is a key measure of quality.[55] The possibility of investing in a collaboration that may or may not have the skilled personnel to carry on the projects in the future is not likely to attract much foreign investment, especially when more qualified, stable technoparks and other SEZs are thriving in Asia.

Additive Manufacturing, aka 3D Printing

Additive manufacturing (AM) or 3D printing technology is a rising industry with applications that traverse all sectors of the economy. A variety of users can use 3D printing commercially or recreationally to make objects in plastic and metal, thus it has caused concern among the security community regarding its potential dual-use capability by states or non-state actors. Despite the concern, current AM capabilities give little cause for alarm. What AM possesses in flexibility, it lacks in depth; AM has limitations in size, material strength, and cost of objects compared to traditional manufacturing methods. The United States and international community should work together to continually examine AM capabilities in the near term and begin to update export control mechanisms, re-examine signatures of proliferation for the intelligence community, and promote collaborative efforts between the AM technical community and the public sector to alert of disruptive ability of the technology.

Background

The onset of what some have called the fourth industrial revolution,[56,57] is marked by technologies that integrate the digital age (third industrial revolution, following steam power and electrification) into society and even the human body. Technologies in the fourth industrial revolution include: artificial intelligence, nanotechnology, advanced robotics, the Internet of Things, and advanced manufacturing capabilities, especially additive manufacturing. In the post-digital age, unprecedented manufacturing techniques are seen as having the potential to alter the current manufacturing paradigm and supply chains.[58,59]

Traditionally, engineers have designed and created products according to subtractive manufacturing techniques, i.e., removing material from a fixed-size object. Economies worldwide have perfected these techniques to optimize the speed and cost of the production of goods. Recent improvements in additive manufacturing, i.e. adding layers to create objects, have risen in the past couple decades. The private sector has capitalized on its use in creating quick prototypes of products, which has given rise to a function-based synonym for 3D printing, rapid prototyping. A 3D printing machine will add layer-by-layer material of some plastic, resin, or metal. Common methods to produce these objects include extrusion (unwinding a wire-shaped feed material), stereolithography (shining light on surface to bond molecules of a liquid polymer together), laser sintering or melting (focusing a laser on metal powder to bond molecules and successively adding powder layers on top). These methods require a computer-aided design (CAD) file as an input; a computer program or the printer itself will deconstruct the image into many cross-sectional layers to be used as steps for the printer.

What are the current capabilities of 3D printers? For commercial 3D printers, they spread the gamut of sizes and prices. The cost ranges from several hundred to a few thousand dollars, and the feed filament costs approximately twenty dollars per kilogram.[60] Most household 3D printers are relatively small, and their application is only relevant to relatively small objects less than half a meter in one dimension.[61] The physical limitations render it useful only for low-quality objects, such as gears, screws, household tools, etc. However, even "household" 3D printers can have resolution up to the sub-millimeter scale. A plethora of websites contains ready-to-print stereolithography (STL) files,[62,63,64] which feed into most 3D printers or allow conversion to a similar format.

Industrial 3D printers, as expected, come with higher costs yet more robust capabilities. The majority owners of higher-tech 3D printers include Department of Energy national laboratories, defense contractors, and large companies such as General Electric and Hewlett Packard. Oak Ridge National Laboratory (ORNL) printed the first-ever 3D printed car, a 2014 Shelby Cobra with their Big Area Additive Manufacturing (BAAM) machine.[65] Lockheed Martin uses additive manufacturing to produce prototypes and parts for satellites and fighter jets; it also operates several AM innovation centers and an AM machine that can print metal objects up to nineteen feet long.[66] Raytheon, another defense contractor, successfully printed the components and assembled a small missile.[67]

The end uses for many commercial and industrial applications include rapid prototyping of objects and making objects that are traditionally difficult to manufacture. Should it be timely and cost-effective, it has the potential to replace staple manufacturing processes such as casting, molding, and forming. Because each layer is added successively with AM as opposed to relying on the hardening or shaping of feed material, orientations that are traditionally challenging to manufacture become either achievable, more efficient, or both. Current 3D printing technology lacks time efficiency on a large scale, therefore the technology is most applicable to rapid prototyping. The Shelby Cobra took six weeks to go from the start of printing to drivable car;[68] most weapons and single-use systems will have a higher threshold for performance. The effort to produce a single sample object requires less effort in machining. Furthermore, even if an actor or organization does not possess the technology, 3D print shops and services, although not ubiquitous, are available.

Additive manufacturing has several implications for U.S. national security. First, 3D printing technology is of dual-use in nature. It can be utilized benevolently to make products such as prosthetics, implants, and car parts, but it can also be used to make potentially harmful objects. For example, an organization called Defense Distributed circulated a design file for a handgun called the Liberator.[69] The State Department asked the organization to recant the file, which prompted Defense Distributed to sue the U.S. State Department stating its violation of several constitutional amendments. The U.S. Government won the case due to its argument's focus on national security.[70] Governments may have difficulty with sensitive objects such as the Liberator because it is challenging to regulate its spread under the International Traffic in Arms Regulations, which aims to limit the proliferation of traditional arms as their proliferation could enable terrorism and proliferation of weapons of mass destruction (WMD).

Because 3D printers maintain the flexibility to print objects of virtually any shape, this new technology requires exploration in its ability and likelihood to impact conflict. For this paper, we will examine how AM may contribute to WMD proliferation. The threat of a rogue state or non-state actor obtaining WMD relies on their ability to secure sensitive chemical, biological, radiological, or nuclear material (CBRN) and to obtain the necessary components. It is hypothesized that AM could disrupt traditional acquisition means of the materials needed to create a WMD. Rather than purchasing the required technology, an actor could print the pieces themselves. An actor must gain knowledge to produce the pieces, but the knowledge to produce pieces via 3D printing is lower than that using traditional manufacturing methods. Design, pre/post processing techniques, and process surveillance are not as labor- or knowledge-intensive with AM, although not to understate the importance of tacit knowledge. Lockheed Martin and other corporations have also demonstrated that techniques such as laser sintering and melting allow production of higher-strength metals.[71,72] The facile procurement of computer files over the Internet permits almost any actor to have access to these files. The files are not so easily detectable, and the end use of the eventual 3D-printed object can be unclear. Evidently, weapons of mass destruction pose a threat to U.S. citizens at home and abroad as well as threaten the security offered by the strategic position of the United States.[73] An easier acquisition of these weapons decreases the significance of the U.S. deterrent threat.

In addition to the relative ease in fabricating machined parts, widespread use of AM could make it difficult to design counter-WMD strategies and further complicate efforts to detect, monitor, and prevent proliferation. It decreases the size of facilities that could be used to create WMD, thereby "rendering detection by international inspectors or national intelligence agencies much harder."[74] AM is touted as a technology that can bring 3D printing to each household, therefore it is not unfathomable to assume that AM weapons production could be dispersed throughout a wider area or in multiple, smaller buildings. This phenomenon could increase the security dilemma for the United States; the probability of successful detection of a covert WMD program decreases and the transparency of weapons manufacturing decreases.

Current thinking on the evolution of additive manufacturing also raises two potential long-term impacts on U.S. security interests: energy efficiency and economic dominance. Increases in energy efficiency maintain positive economic and environmental impacts on the United States; citizens save money and pollution is reduced. Additive manufacturing, as compared to subtractive manufacturing, produces little waste due to the nature of the technology. Subtractive methods can use as little as 5% of the input material whereas the additive methods can use 98% or more of the input material in its final product; additive methods have also been shown to use approximately 50% less energy to produce parts.[75] If these statistics are true, the United States has a lot to gain from this technology. Another potential consequence of international implementation of the technology is that it could reduce the dominance of the United States manufacturing sector. The United States relies on protecting its infrastructure to maintain economic security in international markets.[76] 3D printers could decrease the infrastructure threshold, equalizing the capabilities among states. Both of these claims are of little significance currently as AM has not grown to the scale of traditional manufacturing and thus will not be examined here. Little evidence proves that these are immediate concerns, but the actualization of these speculations could impact long-term U.S. national security.

Prior Work

Little exploration of this technology and its impact on WMD and counter-WMD has been performed. A prominent work detailing the threat of additive manufacturing to the spread of nuclear weapons specifically is a 2015 piece by Kroenig and Volpe,[77] in which the authors assert that 3D printing enables WMD-proliferation because it requires little technical knowledge and potential facilities that could produce WMD-sensitive parts can be widespread and impossible to detect. Although they offer logical conclusions, they simplify the technology without further examining it and how it would be realistically implemented by a WMD-seeking actor and the international regimes that could re-analyze proliferation threats with respect to AM technology. they simply assume that rogue states or non-state actors will covertly pursue the technology. They fail to answer the question of how, i.e., what would a covert AM-driven nuclear WMD program look like?

Another gap in the existing literature is more speculative and draws on comparison to successfully disruptive technologies such as the Internet and personal computers.[78] In both instances, technologies gave informational and entrepreneurial power to the individual. Experts have created analogies between these technologies and additive manufacturing, but they fail to dive past the surface level. They believe that the individual nature of these technologies warranted its success, and therefore additive manufacturing will follow a similar trajectory to that of personal computers. They assume advancements in AM are inevitable and exponential, hence disruptive over a short period. Many articles cite the attention and investment AM has received over recent years, with AM innovation centers surfacing in the United States, Europe, and Asia, as the main indicator of its potential.[79] Some scholars, however, have projected that AM rests at the top of its hype curve and that it requires great technological and institutional demands to overtake traditional manufacturing methods.[80] Some assessments state that "the ability to produce weapons outside traditional fabrication channels also carries additional challenges" yet fail to dig deep into the feasibility and investment necessary to actualize that path.[81]

Other sources have focused on the application of additive manufacturing in the military industrial complex[82] and the spread of 3D-printed traditional munitions.[83] The former does have implications in the speed of the military to actualize a product, while the latter does pose real international security concerns. Both fail to accurately connect these changes to their potential impacts on weapons of mass destruction. The former article states that there are "catastrophic consequences [with] the prospect of additive manufacturing technologies being applied to produce weapons of mass destruction." Generalizations are made about how quantities are lower for successful production and the facilities are easier to hide. There lacks an understanding of the detailed implementation should a state or actor pursue a WMD through these means and which technologies are most sensitive should an actor pursue an AM capability. What facilities should military forces seek and target? How can the international community limit these capabilities through export control? What are indicators of proliferation through this technology?

Current research fails to acknowledge or discredit the role of additive manufacturing as it relates to WMD acquisition by rogue states and non-state actors. Although concessions exist that the technology is not up to par to be viewed as immediately threatening, scholars tend to shortcut to the end point where AM is the ideal disruptive technology due to ideal characteristics that it has yet to currently achieve. A technical breakdown of the technologies is necessary to examine the practical use of the technology to analyze the true threat to U.S. national security interests.

Nuclear Proliferation

The nuclear proliferation threat relies on two main components of the nuclear fuel cycle, enrichment, and reprocessing capabilities. Because highly-enriched uranium can only be produced with enrichment technology and weapons-usable plutonium can only be produced with reprocessing capabilities, these are the technologies of concern for WMD proliferation. Of these two sensitive stages of the nuclear fuel cycle, one must be implemented for the successful acquisition of a nuclear bomb. The exception to that is the case where a fabricated nuclear bomb is stolen, however this risk is not heightened with the advent of advanced manufacturing technologies.

Enrichment capabilities are used to increase the fissile content of natural or low-enriched uranium to weapons-grade uranium. The most current case of uranium enrichment for WMD-seeking purposes is Iran. Based on publicly available data, Iran reportedly had upwards of 19,000 gas centrifuges of the IR-1 to IR-8 models. The models all have similar dimensional orders in terms of eights and diameters, no more than 0.65 meters and no more than 2.5 meters, respectively.[84] With size constraints, these centrifuges could theoretically be 3D printed with a moderately large 3D printer. Components that require the smallest resolution in a gas centrifuge, e.g., two millimeters, such as the molecular pumps and motor stators, could also be made.[85]

A major problem with centrifuges is that they require highly corrosive-resistant materials. Uranium hexafluoride, the form of the uranium in the centrifuge, is highly corrosive to most metals. Maraging steel or strong aluminum alloys is required for rotating components to avoid corrosion; neither of these materials are used extensively outside sophisticated laboratories. Variations of maraging steel and aluminum alloys have been commercially and experimentally listed as below the Nuclear Suppliers Group's (NSG) threshold for ultimate tensile strength necessary for a gas centrifuge component.[86] Even if the strength of the material met NSG standards, exporting it to a non-weapons state would disregard international treaties. If an NSG country wanted to disregard the agreement, it could do so without any consideration or use of AM technology.

In addition to these technical limitations, logistical limitations also exist. The theoretical time required to additively manufacture, assemble, and arrange hundreds or thousands of centrifuges would render it impractical. AM have solely been proven effective, disregarding economics, for small-scale production or prototyping. An actor deciding to pursue these weapons would more likely decide to invest in a "tried and true" method, such as through the experience of the A.Q. Khan network.[87] Furthermore, an enrichment facility requires the cascading, or joining, of hundreds or thousands of centrifuges to increase their utility. Such a facility could likely be detected through surveillance methods, as was the case with the Natanz facility in Iran.[88] A compelling case would be if a new centrifuge configuration could be designed to fit in a smaller space, yet this novelty would not be due to improvements in additive manufacturing.

Reprocessing capabilities, on the other hand, were developed to chemically separate uranium from plutonium in spent nuclear fuel. Reprocessing technology has been the preferred route for several proliferating countries, including the ostensibly-proliferated countries of India, Pakistan, and Israel. The main ingredient in nuclear reprocessing is already-used nuclear fuel. Many processes exist to separate plutonium, but the most widely used is the Purex (plutonium uranium extraction) process. Purex is a solvent extraction method that uses nitric acid to separate plutonium and uranium by their oxidation states.[89] Albeit a straightforward chemical process, Purex implementation requires expertise in nuclear-related disciplines. Nuclear fuel to be reprocessed will be at high levels of radioactivity, therefore advanced hot cells are a necessary technology. Criticality safety experts are needs to ensure subcritical, and therefore nonexplosive, results of the process. Radiation shielding materials, such as concrete, are also required to limit dose to workers at the facility. These materials and expertise are the main barriers to constructing a reprocessing plant with enough throughput to fabricate a plutonium weapon. Slabs of concrete and the complicated, large components for hot cells needed to handle nuclear fuel are not feasible hurdles for AM to surmount. Traditional manufacturing methods have the advantage in this regard; AM would not be worth the financial and knowledge investment to develop a reprocessing facility. This excludes the assumption that an actor has access to a significant quantity of fissile material and therefore must bypass current nonproliferation efforts.

Table 1 shows the risk associated with each sensitive nuclear technology and summarizes the previous few paragraphs into a qualitative chart. It notes that AM adds no risk in obtaining radiological or nuclear material itself. Most technologies fall under the low risk category due to handling of toxic gases or the need to constrain materials in vacuum. The simplest pieces of equipment (end caps, casing, etc.) pose the greatest threat of any technology in the table due to the ability of AM to build pieces with precise specification without excessive bulkiness of the objects. The relative utility of making these pieces with AM has the potential to be marginal, but the flexibility of the machine to make these pieces can increase in the future with suggested improvements in material properties. One could easily produce casing and end caps for centrifuges, as they fit within size constraints, should advance metal AM techniques like laser sintering become commercially available and cost effective.

Chemical Proliferation

The Chemical Weapons Convention identifies three main classes, called Schedules, of controlled substances.[90] Schedule 1 substances have no peaceful use outside chemical weapons while Schedules 2 and 3 substances have small-scale and large-scale uses, respectively, outside chemical weapons. The main substances discussed in this section are sulfur mustard ("mustard gas") and nerve agents, as well as their precursors. Chemical weapons are traditionally difficult to produce due to highly toxic and corrosive chemicals, and their sophistication can vary as evidence of production by the United States, the former Soviet Union, and Iraq.

Sulfur mustard production requires large amounts to be militarily effective. Even if produced in a small quantity, it is difficult to store and transport. It also possesses a relatively low casualty rate, and medical care has developed to ensure increased recovery rates. Its production historically involves ethylene oxide and hydrogen sulfide,[91] both of which are gases at room temperature and therefore difficult to fathom production with AM. The intermediary product between these two chemicals and sulfur mustard is thiodiglycol, which is a common liquid solvent used in ballpoint pen ink and other plastics. It is of interest to private corporations, including Hewlett Packard, who cited it as a functional material in its patent for 3D printing technology in 2017.[92] This patent does not indicate a threat of thiodiglycol production, but it signals interest of using it by private corporations. Without its direct application, exploration of similar chemicals with 3D printing could generate publicly or commercially available knowledge with utilizing it. Therefore, thiodiglycol is a medium risk in the long term, indicated in Table 2. Thiodiglycol requires hydrogen sulfide to produce the sulfur mustard, therefore proliferators need additional anti-corrosive equipment not aided with the use of 3D printing.

The tabun nerve agent poses a similar challenge as the required hydrogen cyanide reagent is necessary.[93] Sarin and soman, other nerve agents, require hydrochloric acid or hydrogen fluoride, both highly corrosive. 3D-printed containers would not withstand storage or transport of these materials. The AM community would need to experiment more with corrosive reactions on mostly metal materials to ensure advantages over steel pipes and containers. Therefore, materials associated with nerve agent production pose a minimal threat. Table 2 shows the relatively small threat that chemical weapons alone pose.

It's been well-recognized that moderately advanced chemical and pharmaceutical industries can enable chemical weapons production.[94,95] Successful acquisition would require conversion of a standard plant to one that could produce chemical weapons. It is therefore possible that AM could be used to create equipment originally intended for a chemical plant that is eventually converted to a chemical weapons facility. An article has proposed effects of current AM technology on the chemical industry to include surgical preparation and drug delivery devices,[96] although both are only projected and have not been demonstrated outside of an experimental setting. Many 3D printing applications for chemical application cross into the biomedical and biotechnology arena.

Biological Proliferation

Biological weapons have overlaps with the production of chemical weapons with a few exceptions. One hypothetically needs to produce a significantly smaller amount of harmful biological material to create the same number of casualties as a chemical weapon. They typically fall into two categories, microbial pathogens or toxins. Most research requires technologically sophisticated facilities capable of examining living organisms at the cell level.

Because of this fact, additive manufacturing adds little to a direct threat from biological weapons. Microbial pathogens such as anthrax, brucellosis, and tularemia, must grow in a controlled environment. Producers of these weapons must ensure sufficient protection of the workers to not infect their own population. Bioprinters are typically designed to work with biocompatible material to make pieces to be inserted in or on the human body.[97] Some research has explored the confinement of small bacteria populations within a hydrogel,[98] but interactions between bacteria and conditions that permit growth of large populations is not well understood. Additive manufacturing adds little to the picture if a sophisticated facility with highly trained experts is required to understand the phenomena itself let alone the fabrication of a weapon. Building up to a larger set of facilities to acquire an operational capability is not facilitated with additive manufacturing.

Openly-published literature about bioprinting is important. Greater transparency in the capability reduces the security dilemma of biological research. Research on development of antibiotic-resistant bacteria does not intersect with advances in additive manufacturing. The area of interest for potential disruptions is genetic engineering, which alone has the potential to create "supergerms" that are highly resistant,[99] notwithstanding overuse of antibiotics.

Current methods to grow biological weapons material with microorganisms involves a seed culture that is fermented. Although advances could improve on growth of microorganism communities, they are not a substitute for the organic material itself. Fermenters for organic culture growth, typically called bioreactors, are complicated machines that are made of stainless steel.[100] Sizes can range from that of a microbial cell (a few square centimeters) to commercial sizes of hundreds to thousands of liters. Smaller sizes have potential to be manufactured with AM, yet supplemental pieces will also be required. This information on AM threats to biological weapons is included with the chemical weapons in Table 2.

Weapons and Delivery Systems

Acquiring the 3D printer capable of missile component production would be difficult. It can be assumed that a missile needs to be manufactured out of high-strength, versatile metals. Even the most advanced equipment has trouble creating these ideal metals. At Lawrence Livermore National Laboratory (LLNL), for example, scientists are running into issues with 3D printing of metals using laser powder bed fusion, currently "the dominant method for producing 3D printed metal structures."[101] The technology is advanced, but this knowledge would be difficult to transfer to less-advanced facilities or poorly equipped actors. Porosity remains an issue for these researchers as they are still trying to understand the science of metal vapor in the process. The scale of their implementation is small, at the millimeter level. Making a full missile solely from AM would be almost an insurmountable technical challenge with today's technology.

The only institutions capable this far of producing some objects for advanced technological systems are the large American corporations. As mentioned earlier, Raytheon 3D printed a missile, but printing spare parts for the satellites is still on the horizon. SpaceX has recently 3D printed a full SuperDraco rocket engine through laser sintering. However, the material used was a superalloy of Inconel, which is several times more expensive than stainless steel. Obtaining access for strong materials necessary for a well-designed weapon remains a hurdle, but one could claim that a state (or sub-state actor) only needs a crude weapon to successfully set off a WMD. It will still need to invest in an additive manufacturing system to meet that goal. Conservative estimates of an AM machine cost are around $500,000.[102] This cost would increase for a potential proliferator given lack of sufficient technical expertise and economic infrastructure to produce necessary components.

Because additive manufacturing is a technology in its early stages of development, it is unlikely that a proliferator will want to pursue two challenging technologies of which they lack expertise if a cheaper alternative to the same or superior (to what they could produce) technology is available. That increases the uncertainty of success as well as the time to acquire the technology. Some ballistic missiles even use solid fuel, but it is not likely that a proliferator would attempt to make fuel with a 3D printer (even if the materials were available) because solid fuel adds more technical and practical knowledge to understand how to manage it. Liquid fuel is almost always preferred, and 3D printing has no advantage with liquids.

Importance of Tacit Knowledge

Some alarmists of the threat of additive manufacturing continue to understate the importance of tacit knowledge in AM, often conceding that some of it is necessary but then assuming that once a piece is finished, it is ready to be used. It is important to note that 3D-printed objects require a fair amount of post-processing. Casting and molding the piece may be irrelevant, but objects are rough coming off of a 3D printer. A delivery system such as a missile or aircraft needs to be finished properly for aerodynamic considerations. Different aerodynamic properties could decrease the accuracy of the weapon, rendering it useless for an actor's mission of destruction should they choose to target a specific location and not wreak general havoc. Grinding, sanding, and polishing would be skills required to bring the object to its intended use. Expertise in that area is still being developed. This is not to say that finishing a 3D printed object requires a significant amount of effort, but it is important for sensitive weapons systems. Welding is another skill that is necessary for AM applications. If a nation wanted to 3D-print a missile, they are most likely going to have to weld materials together. The 3D printers that can print the ORNL Shelby Cobra or a small plane are the highest quality printers in the U.S. infrastructure. It is unlikely a nation to indigenously manufacture a 3D printer of that quality or to buy it from the United States.

Nuclear weapons have an extensive history of proliferation through spread of tacit knowledge as well as technology. The AQ Khan network remains the most infamous nuclear proliferation networks, which contributed to the nuclear weapons acquisition of North Korea.[103] Scholars have also noted the understatement of tacit knowledge in the spread of biological weapons/terrorism.[104] Tacit knowledge is similarly important in 3D printing as machine failures and material wastes can be significant without technical experience. The adoption of 3D printing technology is not simply a matter of detailing scientific or engineering advances to a new process."[105] Tacit knowledge is important in all emerging technologies, including CBRN weapons development. A prominent example includes safety precautions in order to prevent harm to operators; it is challenging to know problems without having operated the equipment before. Safety concerns are of little importance to 3D printers, but economic considerations are important to ensure functionality of a machine with little technical support for proliferators. Communal tacit knowledge by a small group or larger scientific community may not transfer well to a proliferator that can obtain a sophisticated 3D printer. Tacit knowledge highlights the actualization of weapons-usable material after technological acquisition. Equating the two is an invalid assumption.

Analysis and Assessment

Spread of sensitive nuclear technologies is not possible with the technology in the near future. Delivery systems are more worrisome, yet their actualization probability remains low. Additive manufacturing overall poses a miniscule threat of WMD acquisition. CBRN material cannot be produced with 3D printers alone, and the mechanical and chemical processes are challenging with today's technology. Little signs point to a disruptive capability of AM to proliferate WMD to aspirant proliferators. Delivery systems remain the most prevalent opportunity for proliferators to use AM; small yet complex objects like casing or bodies of these systems are ideal candidates for AM pieces. It is important as well to view weapons acquisition with AM through the lens of relative gains compared to traditional manufacturing methods or other means of technological acquisition; proliferators could look to AM or other similar technologies as covert, innovative, and cost-effective ways to increase their power and leverage.

While additive manufacturing is not on the brink of threatening international stability, it would be wise to monitor its progress in the near future. Although 3D-printed missiles or aircraft capable of delivering WMD may not be used next year, the industry is growing rapidly. Currently, there is not a strong need to strictly limit the technology, but with more advances in sensitive areas, AM should be viewed as a dual-use technology. Although detection will be challenging, export controls will need to be enacted to ensure proper end use of the technology.

Due to the potential transferability of files, cybersecurity should be strengthened of organizations, such as defense contractors, that may use this technology for military applications. Understanding of computer design programs is more widespread, and it would be easier for a relatively unskilled actor to print the 3D file. It would also be wise to limit the domestic use of AM for sensitive technologies or to split into multiple files. Saving a 3D file for a centrifuge, for example, is too risky to maintain on a single file. Even if an actor could not 3D print the piece, insight can be gained from the file itself, e.g., specific geometries or supplemental systems. It is possible to entertain the idea of making some of the manufacturing techniques confidential so as the spread of this eventual dual-use technology is curtailed. This action could also aid the U.S. economy should AM become a viable large-scale production method.

An undesired implication of AM is that decreasing transparency of production can potentially worsen the security dilemma. If states do not have a clear picture of what types of materials different states are using to build different types of equipment, it makes it harder to discern whether the produced equipment is inherently defensive or offensive in nature. While this most likely will not be a concern at first since AM is primarily focused on repairs and limited amounts of small munitions, this could become worse as the ability of AM expands to more offensive weapons and military systems. Further research could be pursued to identify how this decrease in transparency could affect the security dilemma. Even though the material inputs are slightly more standardized for 3D printed parts, there are still some specialized materials that must go into the production of weapons systems. Identifying those materials and how they can be tracked should be a priority in the context of understanding the implications of additive manufacturing on U.S. national security.

(Refer to Supporting Data on Page 35)

Machine Learning and Artificial Intelligence

Machine learning leverages large computational power to quickly analyze large amounts of data to produce useful information. While the theory and approaches are decades old, only in more recent years has sufficient computer power become available to make it useful to solve large and complex problems. One of the most remarkable successes of machine learning was the defeat of chess grandmaster Garry Kasparov at the hands of IBMs' Deep Blue chess computer in 1997.[106] Kasparov, the reigning world champion at the time, had defeated Deep Blue a year earlier, losing the first match but developing strategies that exploited the machine learning approach's weaknesses to come back and win the series. In the ensuing year, the algorithms were updated, and more computational power was added; Deep Blue won the series that came down to the final match. The field of machine learning has matured in parallel to increased computation capabilities. Such systems have proven able to solve very complex problems at speeds orders of magnitude faster than humans.

The effective use of machine learning in a military context is not science fiction. The Swedish defense department used machine learning to analyze submarine incursions into its territorial waters in 1986-95.[107] The goal was to learn from patterns of observations and then make future predictions based on incoming intelligence reports. Given the limited data set and the varying reliability of reports, their goals were modest but useful for predicting future events:

A statistical analysis based on a simulation of the method showed that the probability of a correct prediction was at best 54%, with an accuracy in predicted position of 5 kilometers and in predicted time of 48 minutes. Prediction rules with a probability and an accuracy such as these should be very useful if they can be approached in practice.[108]

Contrast this to the earlier application of selecting a chess move, especially near the end of the game when few pieces remain. In the chess example, the moves are deterministic (a pawn attempting to capture a rook legally will capture it 100% of the time), information is complete (the location of each piece is known with 100% accuracy 100% of the time), and the information is completely reliable. Further, the evaluation criteria (win by checkmate while avoiding being checkmated first) are clear and constant.

In security applications, machine learning will have to process incomplete information of various (and unknown) accuracy and validity. Its predictions of behavior will not be deterministic, and even the desired outcomes may sometimes be in doubt. The underlying models may be limited or unknown. This is a very different problem, and expectations must be tempered accordingly.

The machine learning discussed so far is characterized by a computer system manually optimized for the specific indicator analysis required by human experts. It must be provided with properly discretized and verified data to do a specified analysis. This is the realm of the current day and the near future. Despite decades of effort, the "quantum leap" to a generalized AI system has not yet happened.

A generalized AI system, for purposes of this section, is an AI that not only could seek out its own data without specific discretization, formatting, and verification, but also figure out the right sub-questions to ask and do analysis between data sets in unexpected, unprogrammed, perhaps even creative directions. It can take simply stated objective questions and attempt to answer them without much further guidance. It could also ask for data it lacks that it thinks would be valuable in analysis. It is unbounded by processing power or data storage in any meaningful way, and thus can handle any amount of useful data, or filter a very large data stream for useful bits. Most distinctly, it can improve its own analysis in a recursive manner as it works—it need not depend on human programmers past initial setup. Such an AI could make efforts at far fewer binary indicators and analyze situations that lack large data sets or precedents.

The state of the art for imagery analysis is surely classified in the United States. There has been research conducted in open source about using imagery analysis to detect and determine environmental impacts, including excavation.[109]

Advanced Stealth—Meta-Materials

Metamaterials are synthetically manufactured material that possesses special physical properties that allow it to disguise the user from detection. The practical application of metamaterials is to use them to camouflage personnel, vehicles, ships, or planes from some portion of the infrared spectrum. Metamaterials have a high refractive index meaning that light 'flows around' the material rather than reflecting off. Successful implementation of metamaterial adaptive camouflage (MMAC) would be a paradigm shift in camouflage and anti-detection technology which could cause significant disruptions to conflict dynamics. Revisionist actors, as well as non-state actors, will benefit from acquiring a MMAC capability but will struggle to do so due to the technical challenge of advanced R&D. The implication is that status quo powers—whom will be the first to develop a viable capability—must emphasize parallel development of countermeasures and control the diffusion of the technology.

Adaptive camouflage, or active camouflage, is a technology which allows the user to conceal itself from plain sight.[110] Other proposed variants of adaptive camouflage include cloaking from a broader range of the infrared spectrum. Adaptive camouflage technology is currently in the early stages of development and is not deployed in the field. There are prototypes in development including, most promisingly the ADAPTIV Cloak of Invisibility from BAE systems that provides the user with the ability to cloak a vehicle with a honeycomb plating which can adjust the projected appearance and temperature of the vehicle to match the surroundings or mimic another type vehicle.[111] The company claims the technology could be used to conceal anything from trucks to helicopters and even buildings. ADAPTIV conceals the vehicle from IR detection but does not offer plain sight disguise.

Aside from military contractors which are developing adaptive camouflage technology, many artists are also attempting to use existing technology to fashion their own cloaks of invisibility. There are certainly challenges impeding the development of a true cloak of invisibility but most of the informed speculation from the scientific community is cautiously optimistic about the future of adaptive camouflage technology. However, the potential of adaptive camouflage technology can be inferred by examining its scientific foundations.

Adaptive camouflage development is inspired by the biological cloaking systems used by reptiles, amphibians, and fish.[112] The goal of active or adaptive camouflage is to make a person, vehicle, or weapon invisible to enemy much like an animal conceals itself from a predator or prey. Invisibility is achieved by altering either color or luminescence. Scientists believe the best chance for humans to replicate the cloaking capabilities of animals is the development of metamaterials - synthetic materials exhibiting unique properties with respect to refractiveness.[113] Metamaterials, essentially, have the ability to bend electromagnetic radiation - light, radar, infrared - giving the illusion that the material is not present. The earliest serious attempts at creating invisibility cloaks from metamaterials were successful in 2006 when Duke physicist David Smith created a microwave bending metamaterial.[114] Smith's cloak used copper spring resonators and only worked in two dimensions. The concept was advanced by replacing the copper with gold and layering them over a synthetic silk which only interacts with a restricted region of the electromagnetic spectrum (terahertz waves). Synthetic materials composed of gold and silk derive their visual characteristics from their chemical compositions. These materials have a negative refraction index resulting from the materials' variable permittivity and permeability.[115] Ostensibly, the material can rearrange its cellular structure to accommodate varying levels of interaction with electromagnetic spectrum. In essence, manufactured meta-materials woven into a surface can be configured in such a way as to deny interaction with subsets of the electromagnetic spectrum - including light. The surface does not reflect light, rather light flows around the surface like water around a stone in a stream.

The development of metamaterials is still in its infancy and truly is an emerging technology. The materials are expensive to create and there are scalability issues due to limitations in the fabrication process of a large metamaterial surface, fabrication is done the scale of micro- and nano-meters. There is also the challenge of broadening the range of angles at which invisibility is achieved. Currently, the best concepts can only achieve invisibility at viewing angles around 60 degrees from head on, leaving the surface exposed from above and below.[116] In the immediate future, metamaterials are unlikely to be a viable due to the prohibitive expense of manufacturing large amounts of the materials.[117] There are also unanswered questions about the durability cloaks. Would the precisely manufactured surfaces stand up to real world wear and tear? 2D optical carpet designs are composed of precisely woven interdependent magnetic threads that create the illusion of invisibility. In a real world battlefield scenario, particles like dust and sand are constantly barraging and buffeting surfaces. As of now, optical carpets are not robust enough to endure continuous operations. There is also the question of operationalizing the carpet outside of lab perfect environmental conditions: temperature and humidity.

As more research is done on metamaterials, and specifically the mass production metamaterial cloaking surfaces, adaptive camouflage will become a more viable technology. Current R&D efforts are focused on developing metamaterials for primarily medical applications.[118] A shift toward camouflage specific applied R&D will lead to quicker development of metamaterial adaptive camouflage. The basic science behind MMAC is progressing relatively quickly. However, the technology is not advanced enough to do human visual spectrum cloaking, the current capability is limited to a bulky system of IR cloaking which is hardly groundbreaking. In order to be effective in a realistic environment, the applied research stage will have to reduce manufacturing costs and address the environmental challenges facing MMAC.

Environmental challenges suggest two options for the development of a practical metamaterial adaptive camouflage. The manufacture of robust materials that can withstand harsh conditions in the long term, or low-cost materials that can be quickly and affordably applied and re-applied e.g., paint-on camouflage. The primary driver of the prohibitive cost of manufacturing metamaterials is the level of precision required to scale complex three-dimensional structures. Other industries like aerospace and automotive have also struggled with the precision problem and turned to 3D printing as a possible solution. 3D printers normally print precise and complex plastic components which cannot be efficiently produced with a traditional injection mold. Researchers from Duke have begun investigating using special metal 3D printers to produce electromagnetic metamaterials. Their prototypes can produce a unit in a fraction of the time as traditional methods.[119] The method not only makes production easier, it also serves as a catalyst for research collaboration. Instead researchers of spending time replicating a complex manufacturing method every time new research is handed off from another team, they can go straight to production with this method, making the discovery process much faster.

Are meta-materials a disruptive innovation representing a new paradigm in stealth? As of now that answer is clearly no due to the environmental and cost constraints on the technology. However, if the pace of R&D in the field continues to progress rapidly, then MMAC could be a game changer in a few decades. Below are scenarios in which MMAC's have the most potential to disrupt the nature of conflict.

Littoral Waters

One of the major markers of modern state vs. state warfare is the challenge of Anti-Access Area Denial (A2AD). A2AD is the restriction of movement into (A2) and within (AD) the theatre of conflict. A2AD is not a concept in the history of warfare. A common thread in conflict from the Ancient Greeks to modern America is the desire to deny the adversary at longer and longer ranges. However, A2AD is unique in the short-term context because of the fairly unimpeded access enjoyed by the United States following the fall of the Soviet Union. From the early 1990's to the late 2000's the U.S. Navy could move into and within virtually any region and "show the flag." Aircraft carriers give the United States global presence and the ability to project power effectively in a crisis situation.

A2AD is challenging the paradigm through the use of advanced anti-ship missiles—namely the Chinese DF 21 'carrier killer' and Iranian small boat mounted cruise missiles. The two threats present different challenges to the United States. The 'carrier killer' scenario will not be addressed in this paper. The Iranian challenge, however, is on the opposite end of the technological spectrum and may be more closely representative of a challenge from a resurgent Russia. The Iranian Navy has equipped Fast Inshore Attack Craft—speedboats—with anti-ship cruise missiles. The fast boats are relatively inexpensive and therefore a cost-effective means for deterrence through shear saturation. The conventional wisdom is that fast boats would swarm and overwhelm an American ship in the Strait of Hormuz—an artery for global energy transportation. While one or a few cruise missile-equipped fast boats would be no match for an American ship, a swarm could be lethal according to naval wargames.[120] Traditional means for ship to ship combat in this scenario are unfeasible due to cost asymmetry between American Tomahawk cruise missiles and the Iranian fast boats. The navy has investigated the use of lasers and smaller, less expensive missiles as a counter to fast boats. [121]

Metamaterial camouflage could be complicating factor in either of the two A2AD scenarios. In the hands of the United States, the camouflage could potentially ensure freedom of movement into and within the theatre by countering the already precarious Chinese C4ISR capabilities and further complicating Iranian fast boat swarms. Conversely, if the technology were to be utilized by the Chinese or Iranians, the A2AD challenge would be much greater. With the added ability to evade detection of U.S. anti-ship missiles, Chinese vessels would become more brazen in their maneuvers in the South China Sea. Likewise, MMAC would be a force multiplier for Iranian fast boats looking to overwhelm a U.S. ship. The proposed counter measure to fast boats is a ship mounted. Laser guided hellfire missile. Metamaterials could render the laser fire and forget guidance systems ineffective or severely hampered.[122] The Chinese scenario is impacted less by the introduction of MMAC due to the myriad methods of detection in the larger South China Sea theatre.

Border/Trafficking

A second scenario in which metamaterial camouflage could be deadly is in a border and illicit trafficking situation. The volume of movement of people and goods across borders is higher than at any time in human history due to advances in transportation technology and an interconnected global economy. Illicit movement of people, money, weapons, drugs, and other valuable and stolen goods is also at an all-time high. Human and narcotics trafficking from the developing to developed world is a public health and human rights crisis. The International Labor Organization estimates that there are over 20 million victims of human trafficking and the industry generates over $150 billion in revenues each year.[123] The global drug trade generates over $450 billion in revenues each year, much of which is fueling civil conflict and organized crime.[124] Opium from the Golden Triangle in South East Asia and the states of Central Europe as well as cocaine from South American Andes is sold to pay for illegal weapons used in conflicts for control of the drug market. Drug conflict causes civil unrest and sows the seeds for civil conflict. In Afghanistan, Opium stocks the coffers of corrupt politicians and government officials as well as war lords and terrorist organizations like the Taliban. These organizations not only impede local development, but also export terrorism to the developed world.

Although initially metamaterial technology will be available to only the militaries of the most sophisticated countries, it could diffuse to smaller states and non-state actors decades in the future. If a criminal trafficking organization could obtain an invisibility capability, their ability to covertly cross borders with illicit goods would be greatly enhanced. According to the Department of Homeland Security, the United States already struggles to interdict maritime and ground based trafficking efforts. The addition of invisibility further complicates the efforts of border authorities to successfully detect and interdict illicit goods.

Perhaps a more worrying scenario than drugs or people is the trafficking of weapons of mass destruction across borders. A chemical, biological, or nuclear weapon crossing a border or into a protected area of a city in order to attack a high value target would be a dream for a terrorist organization. Metamaterials do not address the majority or the most important WMD countermeasures which do not rely on vision for detection. However, the entire border and diplomatic security paradigm is underpinned by the ability to visually perceive the threat space. In this scenario, the United States has no advantage in having metamaterials but is faced with a significant threat if the technology were to fall into the hands of an actor with both the means to operationalize the technology and motive to use it against high value targets or for trafficking illicit goods.

For great power conflict, the peer/near peer scenario, both actors will both have access to some form of metamaterial technology and use it in primarily in the aerial and maritime environments in conjunction with advanced systems like ships and strike aircraft. The United States will have a temporal advantage over other great powers due to its more sophisticated R&D efforts, but it is assumed that others will eventually gain a capability.

In the near future, challenger actors will gain access to the technology and have the incentive to use it to smuggle illicit goods across both land and maritime borders. The dominant power will also us the technology to counter the smuggling via stealth drone technology. Terrorist and insurgent organizations could also develop a rudimentary metamaterial capability in the far future. This could possibly present the most-dire challenge to status quo, dominant powers.

A policy implication is the importance of controlling access to the technology and restricting it only friendly actors as much as possible. In the long term this is not a viable strategy. However, it can bridge the gap between the time where metamaterial camouflage is developed and the time where appropriate countermeasures to the technology exist. Since the technology does favor challengers of the United States more than the United States as a status quo power, it would be beneficial to emphasize countermeasure development concurrently with the development of the technology itself.

Advances in stealth at the personal and small vehicle level—the areas which metamaterials are most promising—are likely to asymmetrically benefit actors seeking to disrupt U.S. national security through hybrid warfare, terrorism, trafficking, and insurgencies. There are applications where human invisibility would be beneficial for status quo powers—such as covert action and special operations. To mitigate the risk of proliferated metamaterial cloaking, status quo powers should seek to develop counter cloaking technology at a faster pace than cloaking technology and control the diffusion of the technology.

Hypersonics and Directed Energy Weapons

On 1 March 2018, Vladimir Putin announced the Russian ongoing effort to deploy six advanced strategic weapon systems.[125] He asserted that with these systems, Russia aims to reestablish nuclear parity with the United States. Although following the lead of the United States in reducing the size of the strategic arsenal,[126] Moscow is introducing new strategic delivery systems allegedly able to bypass any American deployable defense.

For the Russian president, these advanced weapons systems will offset the current status quo and repristinate the balance of forces between Washington and Moscow as it was before the United States unilaterally withdrew from the anti-ballistic missile treaty and built up anti-missile defense systems in Eastern Europe. In Putin's words: "I deem it necessary to emphasize that Russia's growing military power […] will preserve strategic parity and the balance of forces in the world, which, as is known, have been and remain a key factor of international security." In other words, the new weapons will allow Russia to reestablish the nuclear strategic balance by bypassing the American strategic anti-missile defense systems.

Among the six systems presented, and perhaps the ones creating most concerns, are the hypersonic weapons, because they may be difficult to detect, nearly-impossible to intercept, and will compress the defense and attack time cycle.[127] On the other hand, the American administration seems unimpressed by the advanced strategic weapons showcased by the Russian president. Then-Defense Secretary James N. Mattis observed that "[These new systems] do no impact any need on our side for a change in our deterrent posture" and added "the systems the Russian president talked about are still years away." [128] Echoing Secretary Mattis' statement, Michael Griffin, Undersecretary of Defense for Research and Engineering, declared "the hypersonic weapons greatest impact is as tactical not strategic weapons."[129]

The two systems employing hypersonics are the Kinzhal and the Avanguard. The first, the Kinzhal, is hypersonic missile, purportedly able to combine high speed and maneuverability. The missile is reported to have a range of over 1,200 miles and to be able to strike both ground and naval targets. The missile was first fired in March 11, 2018 from a modified MiG-31BM "Foxhound" in South-West Russia.[130] The combination of maneuverability and speed make the Kinzhal extremely difficult to intercept in operational environments by any defense systems.

The second hypersonic weapons system, the Avanguard, is a gliding vehicle that, according to the Russians, can reach 20 Mach[131] and hit targets in the United States homeland "like a meteorite, like a ball of fire."

Hypersonic glide (or gliding) vehicles (HGV) denote a system that is typically released by an ICBM in the boosting phase, between 50 km to 100 km of altitude to glide to its targets with speed in excess of 5 Mach. HGVs can theoretically maneuver in every stage of the fight and glide at a lower altitude than conventional ICBMs. This makes the detection and interception of the HGV a challenging problem. A weapon system consisting of the complex Avanguard plus ICBM would provide a technical gain and it is a strategic offensive weapon, being designed to strike targets far in enemy's territory.[132] Nonetheless, there are limits and unknowns. The HGV speed decreases during the flight trajectory, tending to zero as it approaches the target. The potential vulnerability of the HGV in the terminal phase, i.e., when the speed is lower, can be mitigated through the addition of boosters. However, this choice will negatively affect the design complexity, the cost, and the aerodynamics of the vehicle. Maneuverability is limited by the HGV's speed. It can be demonstrated that the turning radius is proportional to the square of the vehicle's speed.[133] Although the vehicle glides at lower altitudes than ICBMs, its radar cross-section is likely to be hundreds of times higher than the one of subsonic weapons. The heat management can be problematic. After entering the hypersonic regime, the air surrounding the glider ionizes, reaching temperatures potentially higher than 2000 K. This could damage the vehicle, particularly in correspondence of the tip if a wave-rider design is utilized. And finally, the ICBM used to take the glider to the right altitude is vulnerable in the boosting phase.

The strategic gain of the Kinzhal can be assessed through comparison with the RKV-15 aero-ballistic missile, which are currently deployed on Tupolev Tu-160 strategic bombers.[134] The main difference between the Kinzhal weapons is the ability to maneuver during the flight. However, the maneuverability of the Kinzhal is not a crucial factor able to offset the strategic balance of power for two reasons. First, both the Kinzhal and the RKV-15 are equally vulnerable before being fired, i.e., the must be at less than 300 km from the target. The RVK-15 travels at hypersonic speed, i.e., speeds greater than Mach 5. For this reason, the time to intercept the missile limited to about 3 minutes. This makes the RKV-15 nearly impossible to intercept with the current defensive system, despite using an inertial guiding system. Therefore, the technical advantage is not likely to be translated in a significant gain from a strategic standpoint.

The last of the systems from Putin's address is the Peresvet, a mobile, ground-based directed energy weapon to target drones, and, potentially, small missiles and manned vehicles. The laser entered duty, as an experimental system, with the Russian forces in December 2018 according to the Russian News Agency TASS.[135]

Little direct data is available on the Peresvet combat laser system. According to several analysts, it is most likely deployed to execute air defense and missile defense tasks against drones and cruise missiles in operative environments.[136] This is compatible with the fact that, being a mobile weapon system, the source of energy for the laser is limited (probably to the hundreds of kilowatts). Several reasons have been put forward to justify the development of directed-energy deposition weapons.[137] These include lower cost per shot. The fuel needed to generate the electricity for firing the laser should cost less than a dollar per shot. In contrast, the U.S. Navy's short-range air-defense interceptor missiles can cost hundreds of thousands. Directed energy weapons potential offer faster engagement time and the ability to counter radically maneuvering air targets. Lasers can follow and maintain their beam on radically maneuvering air targets. Such systems also may enable graduated responses that range from warning the adversary to damaging it. These advantages, nonetheless, are counterbalanced by a few shortcomings, including atmospheric absorption. Gases and dust in the atmosphere can absorb and scatter the laser beam, hindering the efficacy of the directed energy weapons. Additionally, the ability of a laser to engage several targets in a short time-scale is limited by the time needed to redirect the weapon and the time the laser must dwell on the target to damage it. Finally, hardened targets may be less vulnerable to lasers in the kilowatts range.

The Peresvet, although constituting an example of technical innovation similar to the AN/SEQ-3 Laser Weapon System, which has been deployed by the U.S. Navy, cannot be categorized as strategic defensive system, because the energy pulse is extremely unlikely to be in the tenth-hundredths of Megawatts range, which is required to intercept incoming strategic ballistic missiles.

There is another area in which directed-energy weapons are likely to proliferate: non-lethal weapons (NLW), which have plausibility for urban and hybrid operations. Non-lethal weapons are not themselves a new or game-changing technology. However, new forms of NLW finally enable a standoff capability previously only available from traditional or lethal systems. These system architectures rely on directed acoustic or electromagnetic energy to achieve a desired effect in their targets, whether personnel or materiel.

NLW can be divided into three broad categories. The first is passive NLW, which would include caltrops, spike strips, counter-traction technologies, and the like. These systems are all similar in that once the NLW has been deployed, it requires no active control to engage or interact with its target. There is no chemical interaction between materials or input of energy necessary as the interactions are instead more traditionally physical. Example architectures include Anti-Traction Technologies (A-TT) or "Super Adhesives" which dramatically reduce and increase friction, respectively. Such systems can be applied to road surfaces or vulnerable components to introduce hazards to enemy equipment operation.[138] Furthermore, Combustion Alteration Technologies (CAT) can prevent traditional combustion processes and therefore stall engines for as long as the compound remains present to inhibit standard operation.[139] Lastly, foam and "entanglement" technologies can prevent physical movement of either materiel or personnel, but are physical-restriction based rather than physiological or chemical.[140] All these NLW are notable for generating effects following active application by the operator. They are almost always inherently reversible; though there is risk of damage should opponents attempt to operate equipment in spite of NLW use (e.g., car crashes due to A-TTs). Passive NLW are also usually counter-materiel in purpose with the intention of making asset operation dangerous or impossible rather than destroying the equipment directly.

The second is active conventional NLW. These compounds either induce reactions (sedative, irritation, nausea, etc.) in humans or cause harm on a molecular level to equipment (liquid metal embrittlement, etc.). Similar to passive NLW, an active input from the original user is not necessary, though the actual non-lethal effects are the result of active interactions between the applied substances and the targets, usually with deeper effects than those of passive NLW. These active systems can include elements from passive NLW such as putting A-TTs into a landmine-like deployment system.[141] Active conventional NLW can also affect both personnel and materiel. Liquid Metal Embrittlement (LME) induces a chemical reaction with dramatically weakens the components of a targeted system, making it either dangerous of impossible to operate. Supercaustics are similar, but instead deteriorate systems and subsystems more directly.[142] On the counter-personnel front, malodorants can discourage human activities in a given region while calmative agents can sedate opponents.[143] Active conventional NLW also include more traditional "riot control" systems such as tear gas or TASERs. These systems all require active user deployment or ongoing interaction and usually cause more explicit chemical, physical, or physiological effects than the passive NLW discussed previously.

The third is directed energy NLW and the primary subject of interest. These systems use either specific electromagnetic (EM) or acoustic means to transmit energy to the target and cause a desired effect. These systems range from strobes to induce confusion to an electromagnetic weapon intended to disable vulnerable electrical equipment. Furthermore, this category of NLW is broad and ranges from area-effect systems such as the Area Denial System (ADS) to more targeted "pulsed energy projectiles" which are directed against single targets.[144] On the counter-personnel front, NLW architectures are usually built around acoustic of electromagnetic energy-transfer means with the intention of causing intense discomfort in opposing personnel. Acoustic systems aim for disorientation or nausea while electromagnetic systems usually aim for inflicting pain with no actual physical harm.[145] However, other electromagnetic systems such as the Low Energy Laser (LEL), Isotropic Radiators, or Visual Stimulation and Illusion (VSI) all instead can cause temporary blindness or disorientation in a target due to the bright flash or strobing (Bucha effect).[146] These NLW can be effectively applied in a defensive position in order to discourage opponent attack. EM counter-materiel NLW are of incredible interest because a targeted electromagnetic signal can damage or disable vulnerable electrical systems.[147] While the electromagnetic pulse (EMP) is the most widely cited form of counter-material NLW, it is at present a difficult effect to produce and control short of detonating a nuclear device.

Non-Lethal weapons may be of utility against and concern regarding proliferation by state actors and in hybrid Warfare scenarios as epitomized by the conflict in Eastern Ukraine. Notably, these paired scenarios are dominated by mechanized or otherwise more-modern forces. As a result, electromagnetic counter-materiel systems are especially useful as they are effective deterrents against military actions. Area-effect counter-materiel NLW can prevent the movement of enemy goods or advanced equipment, such as the missile system used to bring down Malaysian Airlines Flight 17.[148] The conflict in Eastern Ukraine involves both urban elements and open-terrain and long-range vehicle combat and supply lines that are vulnerable or relevant to the conflict.

In terms of urban operations, the physical structures currently offer a degree of shielding from both EM and acoustic NLW, the revolutionary change is that NLW can affect target personnel and materiel without directly compromising the structures housing them. EM and acoustic NLW can hasten the process by implicitly protecting allied forces either by incapacitating opponent personnel or disabling opponent weaponry before damage can be dealt.

Conclusions

> *The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but few calculations beforehand.* – Sun Tzu[149]

Emerging technologies present regional security challenges and may exacerbate (or mitigate) the geo-political, military, energy, and economic challenges in the future to a state or region and the potential impacts on U.S. interests and national security. Deep strategic and practical understanding of the significance of emerging technology and its diffusion as well as extending thinking concerning how science, technology, and inter- and intra-national social relations interact to shape and facilitate management of the changing global security landscape is a pressing need for the 21st Century. Russian technology development at the high end is not the area to focus the majority of the national security attention. It cannot be ignored, but they are slow-followers, if at all.

There are actions, policies, and choices that the United States may elect to pursue that will enable us to remain the leader in science and technology. Many of these are based on lessons from history, as well as being cognizant of what has changed from the 20th Century. Some of the approaches require decisions to invest in science and technology and others require policy changes, or policy where none currently exists, particularly in the context of governance.

The sciences on which these new technologies are and will be based are not likely to come out of industry. Yes, industry will develop and manufacture them. Instead it is the importance of basic research. The focus in the United States should be on basic research at the leading or "bleeding"[150] edge of science. It is the work winning Nobel prizes last decade that will form the basis of developments that will make industry millions and billions this decade and beyond and be the basis of technology developments. We need more 'bleeding edge' research.

In order to transform the current paradigm of incremental and evolutionary improvements of defense acquisition programs and systems, recognition of the need to leap ahead and embrace truly far-sighted concepts as well as foster integrated, multi-disciplinary, and cross-cutting basic research approaches is warranted—such as recent dramatic advances within and at the nexus of nanoscience, materials science, catalysis, supramolecular science, bioinformatics, cellular materials, genomics, proteomics, metabolomics, information sciences, and the cognitive sciences. It's much more important that just funding. It is program management, oversight, and management that is risk tolerant.

At a foundational level, it's all about people. Within the United States, changes in patterns of new business formation, especially high-tech startups, have been observed. Tech-based entrepreneurship is dependent on U.S. research capabilities, institutions, and people. Recent trends as far as tech-based entrepreneurship in the United States are worrisome. Between 1978 and 2012, new business starts declined by 44%.[151]

Historically immigrants have disproportionately contributed to U.S. tech industry and capabilities. E.g., Sergey Brin, co-founder of Google, emigrated from Russia when he was six. Some of the numbers are staggering:

> "Since 1900, immigrants have made up one-third of U.S. recipients of Nobel prizes in chemistry, physics, medicine and economics. Immigrants account for more than one-quarter of the approximately 110,000 patents filed in the United States each year. There are more than 1 million foreign students in U.S. universities, representing about 5% of enrollees and providing an estimated U.S.$39billion annual stimulus to the economy. The United States came to its leading position in science and technology in part because talented immigrants could thrive here. The global nature of U.S. academia seeds connections and

> collaborations that make it stronger.[152] The influx of scientists and engineers fleeing Nazi Germany (including Albert Einstein and computer scientist John von Neumann) remains the most dramatic example."[153]

Science and technology is a strategic asset for American diplomacy and for asserting national power. It is our most valued "soft power" asset. The latest data from the Pew Global Attitudes Project survey from March 2013 shows that more than anything "U.S. science and tech advances" are viewed positively, e.g., ranging from 61% positive in Argentina to 85% in Kenya & Senegal.[154] This should be an area to leverage for diplomacy and U.S. influence. If one analyzes the data specifically among "Middle-East/Conflict Area," (Egypt, Pakistan, Turkey, and Uzbekistan), it's even more dramatic: "Tech/ Science Advances" are cited by 86% as a "reason for liking the U.S." More than anything else. It's 73% cited across all Islamic states surveyed, i.e., Egypt, Pakistan, Turkey, Uzbekistan, Bangladesh, and Indonesia. In South East Asia, 82% of those surveyed looked to America's leadership in science and technology. To pre-emptively counter the criticism that one sometimes encounters: it's not about 'other countries liking us;' it's about leveraging what is most effective, efficient, and likely to be enable paths forward.

By contrast, the view (data) from the United States is basically the inverse; only 32% perceive "Tech/Science Advances" as a major reason for admiring the United States and our leadership globally, which may explain some of the lack of prioritizing this area in terms of foreign policy. Because we do not value or see it, we assume the rest of the world thinks the same.

Reducing the risk from misuse of technology will mean consideration of the highly transnational nature of the critical technology required. Traditional and innovative new approaches to nonproliferation and counter proliferation are important policy elements to reduce the risk of malfeasant application of technology that may enable advanced weapons or make production or dissemination of biochemical agents available to a much wider group of actors. Efforts to strengthen existing international regimes to control transfers of dual-use materials are important.[155] Verification still remains a technical as well as diplomatic challenge. The role of international agreements and cooperative programs in the 21st Century is a contested intellectual and policy field.

One approach that would benefit the United States is reinvigorating science diplomacy. The instruments of science diplomacy include means like MOUs and other official government-to-government interactions: the classic tools of traditional Track I diplomacy. Science diplomacy has perhaps made the biggest impact in foreign policy as a part of Track II diplomatic efforts: informal diplomacy between individuals who are not officially empowered to act on behalf of the state but are acting in accordance with a state's foreign policy goals interact through dialogue, exchanges, cooperative programs, or other means as part of increasing cooperation and transparency or decreasing conflict among states. Track II efforts with nuclear physicists and other scientists during the Cold War are legendary, in the best ways.

In many ways, nuclear diplomacy of the Cold War may be argued as the pinnacle of Track II science diplomacy. Overall, Track II science diplomacy has been an under-utilized tool since then, which may be ironic considering that since the early 1990s, the world has become increasingly technologically-dependent and technology has enabled the spread, at an unprecedented rate, of scientific knowledge, capabilities, and materials globally.

Initiated following the end of the Cold War, a core component of Cooperative Threat Reduction (CTR) efforts aimed at redirecting the offensive or weapons-based knowledge and skill sets of scientists in former Soviet states to defensive or peaceful aims includes Track II science diplomacy. CTR has traditionally and by statute of the public funding focused on reducing the risks from nuclear, biological, and chemical weapons. One can envision a role for science diplomacy beyond the former Soviet states and beyond those weapons as part of pro-active 21st Century Cooperative Threat Reduction; for example, one might imagine a program in partnership with Russia to engage Pakistani and Indian scientists and engineers for cooperative threat reduction from misuse of nanotechnology or synthetic biology. As a model policy leveraging science diplomacy to increase global security, CTR offers opportunities in the diplomatic realm, in the engaging scientists and engineers, and for study by international affairs scholars.

In the 21st Century, major barriers to effective science diplomacy include three major risks: not being relevant, not being strategic, and not being at the table. Science and technology are increasingly complicated and complex. The ability to translate and make relevant the role and importance of science to foreign policy aims is critical. While there are notable exceptions, often this is not best accomplished by active research scientists. It's also not often accomplished well by traditional Foreign Service Officers. In the global information age, there is a critical need for champions and for a cohort of individuals who can bridge across technical and foreign policy arenas.

With respect for the need to be strategic, this potential barrier reflects the need for effective science diplomacy to reach outside of science. Rarely, if ever, does science and technology itself drive foreign policy; the potential national security, economic, or other national- and international-level consequences of the application of science and technology to human endeavors is where science intersects with policy predominantly. Science and technology can be causal, intervening, or determinant factors. The ability to recognize, communicate, and identify nodes for intervention, change, or influence are strategic requirements for effective science diplomacy.

Most international legal and regulatory approaches to technologies and to emerging technologies—robotics, biotechnologies, synthetic genomics, gain of function research, nanotechnology, cognitive neurosciences, hypersonics, AI—are still driven by 20th-Century (or earlier) conceptions and institutions. Past methods for other technologies that do not take into account the international nature of the science and the industry are not adequate. Any international regime or approach must be interdisciplinary in focus, cognizant of the multi-polar post-Cold War world, and appreciate the role of private funders, commercial development, and transnational corporations. To be clear, there's a lot of good in the arms control and nonproliferation existing institutions. Rather, these challenges are primarily political rather than technical. Being able to navigate and affect policy at the interface of science and international affairs is where we have immense value.

The tension between adoption and governance of technology must be considered as part of the balance of power. The utility of treaties may be better viewed as more than only a guarantee against using a weapon. Weapons treaties were never an ironclad guarantee that weapons would not be used. Treaties provide stability, reduce uncertainty; enable dialogue, and are confidence building measures. The utility of weapon prohibition treaties as balancing should not be ignored, not because of an idealized imagination that prohibition effectively and permanently limits proliferation or use of a technology but because the act of meeting, networking, building relationships, and negotiating provides a forum for interacting and addressing underlying issues. From this standpoint, governance approaches should be integral to an integrated military strategy for future capabilities development, not the afterthought that attempts to put the metaphorical genie back in the bottle.

[1] Contact information: Dr. Margaret E. Kosal, Associate Professor, Sam Nunn School of International Affairs, Georgia Institute of Technology, margaret.kosal@inta.gatech.edu; 404-894-9664

Acknowledgements: appreciation to GT students Sara Morrell, Andrew Conant, Wes Stayton, Stefano Terlizzi, and Peter Exline for research assistance.

[2] ADM David E Jeremiah (VCJCS, U.S.N, ret), "Nanotechnology and Global Security," Palo Alto, CA; Fourth Foresight Conference on Molecular Nanotechnology, 9 November 1995.

[3] "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization," Adopted by the Heads of State and Government at the NATO Summit in Lisbon, 19-20 November 2010, http://www.nato.int/strategic-concept/index.html.

[4] Colin Gray, *Another Bloody Century: Future Warfare,* London, UK: Phoenix, 2007, p 38.

[5] Defense Science Board, *2006 Summer Study on 21St Century Technology Vectors*, February 2007, 4 volumes, (http://www.acq.osd.mil/dsb/reports/2006-02-Summer_Study_Strategic_Tech_Vectors_Vol_I_Web.pdf & http://www.acq.osd.mil/dsb/reports/2006-02-Summer_Study_Strategic_Tech_Vectors_Vol_II_Web.pdf).

[6] Vannevar Bush, "Science: The Endless Frontier," (United States Government Printing Office, Washington: July 1945) (http://www.nsf.gov/od/lpa/nsf50/vbush1945.htm).

[7] Yong Qin, Xudong Wang & Zhong Lin Wang, "Microfibre–nanowire hybrid structure for energy scavenging," *Nature,* 2008, 451, pp 809–813, https://www.nature.com/articles/nature06601; Carlos García Núñez, Libu Manjakkal & Ravinder Dahiya, "Energy autonomous electronic skin," *npj Flexible Electronics,* 2019, 3:1, pp 1-24, https://www.nature.com/articles/s41528-018-0045-x; Minbaek Lee, Chih-Yen Chen, Sihong Wang, Seung Nam Cha, Yong Jun Park, Jong Min Kim, Li-Jen Chou, Zhong Lin Wang, "A Hybrid Piezoelectric Structure for Wearable Nanogenerators," *Advanced Materials,* 2012, 24, pp 1759-1764; Rusen Yang, Yong Qin, Liming Dai & Zhong Lin Wang, "Power generation with laterally packaged piezoelectric fine wires," *Nature Nanotechnology,* 2009, 4, pp 34-39.

[8] *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern*, 29 March 2012, http://www.phe.gov/s3/dualuse/Documents/us-policy-durc-032812.pdf

[9] F Seitz and RD Nichols, *Research and Development and the Prospects for International Security*, Crane, Russak & Company, Inc: New York, 1973; M Van Creveld, *Command in War*, Harvard University Press: Cambridge, 1985; SP Rosen, *Winning the Next War: Innovation and the Modern Military*, Cornell University Press: Ithaca, 1991; EB Skolinikoff, *The Elusive Transformation: Science, Technology, and the Evolution of International Politics*, Princeton University Press: Princeton, 1993; E Solingen, *Scientists and the State: Domestic Structures and the International Context*, University of Michigan Press: Ann Arbor, 1994; Metz, Steven and Kievit, James. "Strategy and the Revolution in Military Affairs: From Theory to Policy," *Strategic Studies Institute*. 27 June 1995; J Arquilla, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND Corporation: Santa Monica, 2002; PM Cronin (ed), *Impenetrable Fog of War: Reflections on Modern Warfare and Strategic Surprise*, Praeger Security International: Westport CT, 2008; and S Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*, Princeton University Press: Princeton. 2004; TG Mahnken, *Uncovering Ways of War: U.S. Intelligence and Foreign Military Innovation, 1918–1941*, Cornell University Press: Ithaca, 2009; and ME O'Hanlon, *The Science of War*, Princeton University Press: Princeton, 2009.

[10] For example, an incomplete selection includes FA Long and J Reppy (eds), *The Genesis of New Weapons: Decision Making for Military R&D*, Pergamon Press: New York, 1980; G Spinardi,

"Defence Technology Enterprises: A Case Study in Technology Transfer," *Science and Public Policy*, 1992, 19, pp 198-206; H Gusterson, "A Pedagogy of Diminishing Returns: Scientific Intuition Across Three Generations of Nuclear Weapons Science," in D Kaiser (ed), *Pedagogy and the Practice of Science: Historical and Contemporary Perspectives*, MIT Press: Cambridge, MA, 2005, pp 75-107; J Reppy, "Managing Dual-Use Technology in an Age of Uncertainty," *The Forum*, 2006, 4, article 2; BC Hacker and M Hacker, *American Military Technology: The Life Story of Technology*, Johns Hopkins Press: Baltimore, 2006.

[11] SJ Blank, "The Soviet Strategic View: Ogarkov on the Revolution in Military Technology," *Strategic Review*, Summer 1984, 12, pp 3-90; DR Herspring, "Nikolay Ogarkov and the Scientific-Technical Revolution in Soviet Military Affairs," *Comparative Strategy*, 1987, 6, pp 29-59; WJ Perry, "Desert Storm and Deterrence," *Foreign Affairs*, Fall 1991, 70, pp 66-82; AF Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest*, Fall 1994, 37, pp 30-42; J McKitrick, J Blackwell, F Littlepage, G Kraus, R Blanchfield, and D Hill, "The Revolution in Military Affairs," in BR Schneider and LE Grinter (eds), *Battlefield of the Future: 21st Century Warfare Issues*, Air University Press: Maxwell AFB, AL, 1995; JS Nye, Jr and WA Owens, "America's Information Edge," *Foreign Affairs*, March-April 1996, 75, pp 20-36; EA Cohen, "A Revolution in Warfare," *Foreign Affairs*, March-April 1996, 75, pp 37-54; J Arquilla and SM Karmel, "Welcome to the Revolution … In Chinese Military Affairs," *Defense & Security Analysis*, December 1997, 13, pp 255-269; AH Bernstein and M Libicki, "High-Tech: The Future Face of War? A Debate," *Commentary*, January 1998, 105, pp 28-31; FW Kagan, "High-Tech: The Future Face of War? A Debate," *Commentary*, January 1998, 105, pp 31-34; J Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military*, *Ivan R. Dee*: Lanham, MD, 2003; TG Mahnken and JR FitzSimonds "The Limits of Transformation: Officer Attitudes toward the Revolution in Military Affairs**,"** Naval War College Newport papers no. 17, 2003, DoD Office of Force Transformation, *Military Transformation: A Strategic Approach*, November 2003; EO Goldman and TG Mahnken (eds), *The Information Revolution in Military Affairs in Asia*, Palgrave Macmillan: New York, 2004; AA Nofi, *Recent Trends in Thinking About Warfare*, The CNA Corporation, September 2006, http://www.cna.org/documents/D0014875.A1.pdf; and TG Mahnken, *Technology and the American Way of War Since 1945*, Columbia University Press: New York, 2010.

[12] WS Lind, "Defending Western Culture," *Foreign Policy*, Fall 1991, 84, pp 41-50; WS Lind, K Nightingale, JF Schmitt, JW Sutton, and GI Wilson, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, October 1989, pp 2-11; TX Hammes, "The Evolution of War: The Fourth Generation," *Marine Corps Gazette*, 1994, pp 35-41; WS Lind, "Understanding Fourth Generation War," *Military Review*, September-October 2004, 84, pp 12-16; GS Katoch, *Fourth Generation War: Paradigm For Change*, Master's Thesis, Naval Postgraduate School, Monterey, California, June 2005, http://handle.dtic.mil/100.2/ADA435502; JW Bellflower, "4th Generation Warfare," *Small Wars Journal Magazine*, February 2006, 4, pp 27-33; TX Hammes, *The Sling and the Stone: On War in the 21st Century*, Zenith Press: Minneapolis MN, 2006; TX Hammes, "Fourth Generation Warfare Evolves, Fifth Emerges," *Military Review*, May-June 2007, pp 14-21; T Benbow, "Talking 'Bout Our Generation? Assessing the Concept of 'Fourth-Generation Warfare,'" *Comparative Strategy*, March 2008, 27, pp 148-163; MJ Artellia and RF Deckrob, "Fourth Generation Operations: Principles for the 'Long War'," *Small Wars & Insurgencies*, June 2008, 19, pp 221-237; JF McKenzie, Jr., "Elegant Irrelevance: Fourth Generation Warfare," *Parameters*, Autumn 1993, pp 51-60 and JA Echevarria, *Fourth Generation War and Other Myths*, November 2005, Strategic Studies Institute, U.S. Army War College, Carlisle, PA.

[13] Hagel, Chuck. "Defense Innovation Days," Speech at Southeastern New England Defense Industry Alliance delivered by Secretary of Defense Chuck Hagel, Newport, Rhode Island, 3 September 2014 http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1877.

[14] Work, Bob. "Reagan Defense Forum: The Third Offset Strategy," Speech at Reagan Presidential Library delivered by Deputy Secretary of Defense Bob Work, Simi Valley, CA, 7 Nov 2015 https://www.defense.gov/News/Speeches/Speech-View/Article/628246/reagan-defense-forum-the-third-offset-strategy/.

[15] Ellman, Jeesee, Lisa Samp, and Gabriel Coll. "Assessing the Third Offset Strategy," *Center for Strategic and International Studies* March 2017.

[16] National Research Council. "Persistent Forecasting of Disruptive Technology," *Committee on Forecasting Future Disruptive Technologies*. Washington DC: The National Academies Press, 2010.

[17] National Research Council, *Globalization, Biosecurity, and the Future of the Life Sciences*, National Academies Press, Washington D.C., 2006.

[18] "George F. Kennan on Organizing Political Warfare," April 30, 1948, History and Public Policy Program Digital Archive, Obtained and contributed to CWIHP by A. Ross Johnson. Cited in his book Radio Free Europe and Radio Liberty, Ch1 n4—NARA release courtesy of Douglas Selvage. Redacted final draft of a memorandum dated May 4, 1948, and published with additional redactions as document 269, FRU.S., Emergence of the Intelligence Establishment. https://digitalarchive.wilsoncenter.org/document/114320

[19] Geoffrey Chapman, Hassan Elbahtimy & Susan B. Martin (2018) "The Future of Chemical Weapons: Implications from the Syrian Civil War," *Security Studies*, DOI: 10.1080/09636412.2018.1483640

[20] Ion Mihai Pacepa, *Disinformation* (Washington, D.C.: WND Books, 2013), Kindle Location 814.

[21] Marquis de Custine, *Journey for Our Time: The Russian Journals of Marquis de Custine* (Washington, D.C: Gateway Editions, 1987), 14.

[22] Dima Adamsky, "Cultural Underpinnings of Current Russian Nuclear and Security Strategy," in *Crossing Nuclear Thresholds: Leveraging Sociocultural Insights into Nuclear Decision-making*, eds. Jeannie L. Johnson, Kerry M. Kartchner, and Marilyn J. Maines, (Cham, Switzerland, Palgrave Macmillan; 2018); Margaret E. Kosal, "Military Applications of Nanotechnology: Implications for Strategic Security I," PASCC Final Report, December 2014.

[23] Fritz W. Ermarth, "Russian Strategic Culture in Flux: Back to the Future?" in *Strategic Culture and Weapons of Mass Destruction: Culturally Based Insights into Comparative National Security Policymaking*, eds. Jeannie L. Johnson, Kerry M. Kartchner, Jeffrey A. Larsen, (New York, Palgrave Macmillan; 2009).

[24] Stephen Covington, The Culture of Strategic Thought (Cambridge: Belfer Center, 2016). 39.

[25] Carl Kaysen, Robert S. McNamara, and George W. Rathjen, "Nuclear Weapons After the Cold War," *Foreign Affairs*, Fall 1991, 70 (4), pp 95-110.

[26] Robert S. McNamara and James G. Blight, "In from the Cold: A New Approach to Relations with Russia and China," *World Policy Journal,* 2006, 18(1) p. 72.

[27] Jack L. Snyder, The Soviet Strategic Culture: Implications for Limited Nuclear Operations, R-2154–AF (Santa Monica, CA, Sept. 1977); Colin S. Gray, 'National Style in Strategy: The American Example,' International Security, 6 (1981), pp. 21–47; Alastair Iain Johnston, 'Thinking about Strategic Culture,' International Security, 19 (1995), pp. 36–43.

[28] Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies,* 29(5), 2006, pp. 905-934.

[29] Dima Adamansky, The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the U.S., and Israel, Stanford University: Stanford, 2010,

[30] Dima Adamansky, The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the U.S., and Israel, Stanford University: Stanford, 2010, p. 10.

[31] Dima Adamansky, The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the U.S., and Israel, Stanford University: Stanford, 2010, p. 17.

[32] Matthew Evangelista, Innovation and the Arms Race: How the United States and the Soviet Union Develop New Military Technologies, Cornell University: Ithaca, 1988, pp. 26.

[33] Matthew Evangelista, Innovation and the Arms Race: How the United States and the Soviet Union Develop New Military Technologies, Cornell University: Ithaca, 1988, pp. 30-49.

[34] Matthew Evangelista, Innovation and the Arms Race: How the United States and the Soviet Union Develop New Military Technologies, Cornell University: Ithaca, 1988, pp. 52-53.

[35] Adam N. Stulberg, Michael D. Salomone, Managing Defense Transformation: Agency, Culture and Service Change, Routledge, 2007.

[36] Adam N. Stulberg, *Russia and the Nanotechnology Revolution: Looking Beyond the Hype*; PONARS Eurasia Policy Memo No. 26, August 2008, http://www.ponarseurasia.com/sites/default/files/policy-memos-pdf/pepm_026.pdf.

[37] Admiral V. Tributs, "To Develop the Theory of Soviet Military Art," Voyennaya Mysl (Military Thought), October 1960, https://www.cia.gov/library/readingroom/docs/DOC_0000012329.pdf; Colonel-General A. Badazhanyan, "The Nature of Modern Warfare," Voyennaya Mysl (Military Thought), January 1961, https://www.cia.gov/library/readingroom/docs/DOC_0000012316.pdf

[38] Colonel-General Aleksey Ivanovich Radziyevskiy, "Surprise in Starting a War," June 27, 1968, Voyennaya Mysl (Military Thought), https://www.cia.gov/library/readingroom/docs/DOC_0001199077.pdf.

[39] Yu.V.Andropov, "Report Made at the KGB Party Caucus Meeting, By the Member of the CPSU Central Committee's Politbureau, Chairman of the Committee for the State Security of the U.S.SR, KGB, March 25, 1981, https://nsarchive2.gwu.edu//dc.html?doc=5028353-Document-01-KGB-Chairman-Yuri-Andropov-to-KGB.

[40] Jacob W Kipp, "Confronting the RMA in Russia," Military Review, vol. 77, no. 3, (May/June 1997), pp. 49-55., https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/244571.

[41] Kipp, "Confronting the RMA."

[42] Slavo Radosevic, "Patterns of Preservation, Restructuring, and Survival: Science and Technology in Russia in post-Soviet era," 2003, *Research Policy*, 32, pp 1106

[43] Slavo Radosevic, "Patterns of Preservation, Restructuring, and Survival: Science and Technology in Russia in post-Soviet era," 2003, *Research Policy*, 32, pp. 1106

[44] Alexander Uvarov and Evgeniy Perevodchikov The Entrepreneurial University in Russia: from Idea to Reality, Procedia - Social and Behavioral Sciences, Volume 52, 2012, pp 45-51.

[45] A. I. Terekhov, "Evaluating the performance of Russia in the research in nanotechnology," Journal of Nanoparticle Research, November 2012, 14:1250.

[46] Paul H. Nitze "Assuring Strategic Stability Stability in an era of Detente" 1976. Found in Snyder, Jack L. *The Soviet Strategic Culture. Implications for Limited Nuclear Operations*. Vol. 2154, no. AF, Rand Corporation, Santa Monica, 1977, p 25.

[47] Stephen Covington, *The Culture of Strategic Thought* (Cambridge: Bel1fer Center, 2016). 12.

[48] OECD Science, Technology, and Industry Outlook 2012 "*Organization for Economic Co-operation and Development*, 2012, pp 368.

[49] A. I. Terekhov, "Evaluating the performance of Russia in the research in nanotechnology," *Journal of Nanoparticle Research*, 2012, 14(11), article: 1250, pp 10-11.

[50] Itzhak Goldberg, John G. Goddard, Samita Kuriakose, and Jean-Louis Racine, "Igniting Innovation: Rethinking the Role of Government in Emerging Europe and Central Asia," *The World Bank*, 2011, p 83.

[51] Russian Federal law "About special economic zones in Russian Federation (Об особых экономических зонах в Российской Федерации)," 22 July 2005.

[52] Itzhak Goldberg, John G. Goddard, Samita Kuriakose, and Jean-Louis Racine, "Igniting Innovation: Rethinking the Role of Government in Emerging Europe and Central Asia," *The World Bank*, 2011, p 96.

[53] Uvarov Alexander & Perevodchikov Evgeniy, "The entrepreneurial university in Russia: from idea to reality," *Social and Behavioral Sciences*, 2012, 52, p 47.

[54] Itzhak Goldberg, John G. Goddard, Samita Kuriakose, and Jean-Louis Racine, "Igniting Innovation: Rethinking the Role of Government in Emerging Europe and Central Asia," *The World Bank*, 2011, p 105.

[55] J.Q. Trelewicz, "An Analysis of Technology Entrepreneurship in the Modern Russian Economy exploring SEZ, Technoparks,

and the Skolkovo Program," *IEEE International Technology Management Conference*, 2012, p 290.

[56] K. Schwab. *The Fourth Industrial Revolution*. World Economic Forum. 2016.

[57] J. Bloem et al. "The Fourth Industrial Revolution: Things to Tighten the Link Between IT OT." VINT Research Report, Sogeti. 2014.

[58] I. Petrick and T. Simpson. "3D Printing Disrupts Manufacturing." *Research-Technology Management*. 56,6:12-16. 2015.

[59] T. Campbell and O. Ivanova. "Additive Manufacturing as a Disruptive Technology: Implications of Three-Dimensional Printing." *Technology & Innovation*. 15,1:67-79. 2013.

[60] "Price compare—3D printing materials—Filament." Web. www.3ders.org . April 2017.

[61] "3D Printing Materials: Printing Sizes." i.materialise. Web. https://i.materialise.com/3d-printing-materials/printing-sizes. April 2017.

[62] http://www.thingiverse.com/

[63] https://www.youmagine.com/

[64] https://www.tinkercad.com/

[65] R. Jackson et al. "Overview of the Oak Ridge National Laboratory Advanced Manufacturing Integrated Energy Demonstration Project: Case Study of Additive Manufacturing as a Tool to Enable Rapid Innovation in Integrated Energy Systems." ASME 2016 International Mechanical Engineering Congress and Exposition. Volume 14. November 2016.

[66] "By the Numbers: 3-D Printing at Lockheed Martin." *Lockheed Martin*. 2015. Web. =

[67] "To Print a Missile: Raytheon Research Points to 3-D Printing for Tomorrow's Technology." *Raytheon*. April 2016. Web. http://www.raytheon.com/news/feature/3d_printing.html

[68] "3D Printed Shelby Cobra." Oak Ridge National Laboratory. Web. http://web.ornl.gov/sci/manufacturing/shelby/. April 2017.

[69] "Cody Wilson, Who Posted Gun Instructions Online, Sues State Department." *The New York Times*. May 2015. Web. http://www.nytimes.com/2015/05/07/us/cody-wilson-who-posted-gun-instructions-online-sues-state-department.html?_r=0

[70] "Defense Distributed vs. United States Department of State." *Harvard Law Review*. Fifth Circuit 2016. Web. https://harvardlawreview.org/2017/04/defense-distributed-v-united-states-department-of-state/. April 2017.

[71] http://www.lockheedmartin.com/us/what-we-do/emerging/advanced-manufacturing/additive-manufacturing.html

[72] P. Jain, P. Pandey, & P. Rao. International Journal of Advanced Manufacturing Technology (2009) 43: 117. doi:10.1007/s00170-008-1682-3

[73] The U.S. National Security Strategy. February 2015. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

[74] M. Kroenig and T. Volpe. "3-D Printing the Bomb? The Nuclear Nonproliferation Challenge." *The Washington Quarterly*. Fall 2015. https://twq.elliott.gwu.edu/sites/twq.elliott.gwu.edu/files/downloads/TWQ_Fall2015_Kroenig-Volpe.pdf

[75] "How 3D Printers Work." *U.S. Department of Energy*. June 2014. Web. http://www.energy.gov/articles/how-3d-printers-work

[76] D. Gress & R. Kalafsky. "Geographies of production in 3D: Theoretical and research implications stemming from additive manufacturing." *Geoforum*. 60: 43-52. March 2015.

[77] M. Kroenig & T. Volpe. "3-D Printing the Bomb? The Nuclear Nonproliferation Challenge." The Washington Quarterly. 38:3. pp. 7-19.

[78] C. McNulty et al. "Toward the Printed World: Additive Manufacturing and Implications for National Security." *Institute of National Strategic Studies, National Defense University*.

[79] D. Lothringer et al. "Countering Weapons of Mass Destruction: a Preliminary Field Study in Improving Collaboration." *Naval Postgraduate School*. 2016.

[80] Y. Huang et al. "Additive Manufacturing: Current State, Future Potential, Gaps and Needs, and Recommendation." *Journal of Manufacturing Science and Engineering*. 137. 1. February 2015.

[81] D. Tirone & J. Gilley. "Printing power: 3-D printing and threats to state security." *Journal of Policing, Intelligence, and Counter Terrorism*." 10:2, 102-119. November 2015.

[82] J. Mattox. "Additive Manufacturing and its Implications for Military Ethics." *Journal of Military Ethics*. 12. 3. 225-234. 2013.

[83] G. Walther. "Printing Insecurity? The Security Implications of 3D-Printing Weapons." *Journal of Science and Engineering Ethics*. 21. 1435-1445. 2015.

[84] D. Albright. "Technical Note: Making Sense out of the IR-8 Centrifuge." *Institute for Science and International Security*. September 2014. Web. http://isis-online.org/uploads/isis-reports/documents/IR8_Sept__2014.pdf

[85] "Guidelines for Nuclear Transfers." *Nuclear Suppliers Group*. June 2015. Web. http://www.nuclearsuppliersgroup.org/images/Files/Updated_control_lists/Bariloche/NSG_Part1Rev.13_clean.pdf

[86] D. Manfredi et al. "From Powders to Dense Metal Parts: Characterization of a Commercial AlSiMg Allow Processed Through Direct Metal Laser Sintering." *Materials*. 2013, 6, 856-869. http://www.mdpi.com/1996-1944/6/3/856

[87] D. Albright & C. Hindenstein. "Unraveling the AQ Khan and future proliferation networks." *The Washington Quarterly*. 28, 2. 2005.

[88] "Natanz Enrichment Complex." *Nuclear Threat Initiative*. Web. http://www.nti.org/learn/facilities/170/

[89] M. Zenter, G. Coles, & R. Talbert. "Nuclear Proliferation Technology Trends Analysis." *Pacific Northwest National Laboratory*. PNNL-14480. September 2005.

[90] "Annex on Chemicals." *Organisation for the Prohibition of Chemical Weapons*. https://www.opcw.org/chemical-weapons-convention/annexes/annex-on-chemicals/schedule-1/

[91] "Toxicological Profile for Sulfur Mustard." Agency for Toxic Substances & Disease Registry, Center for Disease Control. September 2003.

[92] J. Abbott et al. "Three-dimensional (3D) printing." Hewlett Packard Development Company, L.C. WO Patent App. PCT/ U.S.2015/041,961. February 2017.

[93] "Technologies Underlying Weapons of Mass Destruction." *United States Office of Technology Assessment*. December 1993. OTA-BP-ISC-115. Washington, D.C: U.S. Government Printing Office.

[94] "Chemical and Biological Weapons: The Poor Man's Bomb." *Federation of American Scientists, Intelligence Resource Program*. https://fas.org/irp/threat/an253stc.htm. October 1996.

[95] J. Tucker. «Verification provisions of the Chemical Weapons Convention and their relevance to the Biological Weapons Convention.» Biological Weapons Proliferation. Reasons for Concern, Courses of Action. Stimson Center Report 24 (1998).

[96] B. Gross et al. "Evaluation of 3D Printing and Its Potential Impact on Biotechnology and the Chemical Sciences." Anal. Chem., 2014, 86 (7), pp 3240–3253. January 2014.

[97] Y. Nishiyama. "Development of a Three-Dimensional Bioprinter: Construction of Cell Supporting Structures Using Hydrogel and State-Of-The-Art Inkjet Technology." *Journal of Biomechanical Engineering*. 131, 3. December 2008.

[98] J. Connell et al. "3D printing of microscopic bacterial communities."

[99] C. YanAm & L. Mei. "Get to know supergerms better." *Chinese Journal of Dermatovenerology*. 24:1081-1083. 2010.

[100] "Technologies Underlying Weapons of Mass Destruction." United States Office of Technology Assessment. December 1993. OTA-BP-ISC-115. Washington, D.C: U.S. Government Printing Office.

[101] M. Matthews et al. "Denudation of metal powder layers in laser powder bed fusion process." *Acta Meterialia*. 114. 33-42. 2016.

[102] D. Thomas & S. Gilbert. "Costs and Cost Effectiveness of Additive Manufacturing: A Literature Review and Discussion." *Applied Economics Office Engineering Laboratory, National Institute of Standards and Technology*. December 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1176.pdf

[103] A. Montgomery. "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network." *International Security*. 30. pp 153-187. Fall 2005.

[104] J. Revill & C. Jefferson. "Tacit knowledge and the biological weapons regime." Sci Public Policy (2014) 41 (5): 597-610.

[105] Hoskins, S. (2014) Issues of tacit knowledge within 3D printing for artists, designers and makers. NIP & Digital Fabrication Conference, 2014 (30). pp. 426-431.

[106] Monty Newborn, *Kasparov versus Deep Blue: Computer Chess Comes of Age* (New York: Springer-Verlag, 1997), preface.

[107] Ulla Bergsten, et al., "Applying Data Mining and Machine Learning Techniques to Submarine Intelligence Analysis," Proc. Third Int. Conf. Knowledge Discovery and Data Mining (KDD 1997), 127-130. https://arxiv.org/ftp/cs/papers/0305/0305022.pdf.

[108] Ulla Bergsten, et al., "Applying Data Mining and Machine Learning Techniques to Submarine Intelligence Analysis," Proc. Third Int. Conf. Knowledge Discovery and Data Mining (KDD 1997), 129, https://arxiv.org/ftp/cs/papers/0305/0305022.pdf.

[109] George P. Petropoulos, et al., "Change detection of surface mining activity and reclamation based on a machine learning approach of multi-temporal Landsat TM imagery," *Geocarto International* (2012), https://www.researchgate.net/publication/254237749_Change_detection_of_surface_mining_activity_and_reclamation_based_on_a_machine_learning_approach_of_multi-temporal_Landsat_TM_imagery.

[110] Behold the Octopus-Inspired Adaptive Camouflage, Charles Choi , http://www.popularmechanics.com/science/animals/a11105/behold-the-octopus-inspired-adaptive-camouflage-17108661/

[111] ADAPTIV - Cloak of Invisibility, http://www.baesystems.com/en-us/feature/adativ-cloak-of-invisibility

[112] Stuart-Fox, Devi, and Adnan Moussalli. «Camouflage, Communication and Thermoregulation: Lessons from Colour Changing Organisms.» Philosophical Transactions: Biological Sciences 364, no. 1516 (2009): 463-70. http://www.jstor.org/stable/40485810.

[113] Greenleaf, Allan, Yaroslav Kurylev, Matti Lassas, and Gunther Uhlmann. «Cloaking Devices, Electromagnetic Wormholes, and Transformation Optics.» SIAM Review 51, no. 1 (2009): 3-33. http://www.jstor.org/stable/20454192.

[114] Metamaterials History - people.ee.duke.edu/~drsmith/metamaterials/metamaterials_history_4.htm

[115] Jose Manuel Alves, Metamaterials with Negative Permeability and Permittivity: Analysis and Application, Lisboa Instituto Superior Technico Disseration (2010)

[116] G. Dolling, M. Wegener, C. M. Soukoulis, and S. Linden, «Negative-index metamaterial at 780 nm wavelength,» Opt. Lett. (2007)

[117] Zhang et. al, Demonstration of Near-Infrared Negative-Index Materials, Center for High Technology Materials and Department of Electrical and Computer Engineering, University of New Mexico, Arxiv (2005).

[118] Metamaterials for Medical Imaging, http://www.metamaterialscenter.com/applications/imaging/

[119] Xie et. al, Microwave metamaterials made by fused deposition 3D printing of a highly conductive copper-based filament, Applied Physics Letters Vol 110 Issue 18 (2007)

[120] Millennium Challenge 02. United States Joint Forces Command. 2002. http://web.archive.org/web/20070928005405/http:/www.jfcom.mil/about/experiments/mc02.htm

[121] America's Master Plan to Crush Iranian Warships. Zachary Keck. The National Interest. 2015. http://nationalinterest.org/blog/the-buzz/americas-master-plan-crush-iranian-warships-13602

[122] Methods and systems for optical focusing using negative

index metamaterial. U.S. Patent 8180213 B2. May 2012. A. Young, D. Barker, and W. Owens.

[123] New ILO Global Estimate of Forced Labour: 20.9 million victims, International Labor Organization. 2012. http://www.ilo.org/global/about-the- ilo/newsroom/news/ WCMS_182109/lang--en/index.htm

[124] Drug Trafficking. United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/drug-trafficking/

[125] Vladimir Putin, "Presidential Address to the Federal Assembly," President of Russia, Events, March 1, 2018, Accessed December 14, 2018, http://en.kremlin.ru/events/president/transcripts/messages/56957.

[126] U.S. Department of State, "New Start Treaty at a Glance," Accessed December 14, 2018, https://www.state.gov/t/avc/newstart/.

[127] Richard H. Speier, George Nacouzi, Carrie A. Lee, Richard M. Moore, "Hypersonic Missile Nonproliferation, Hindering the Spread of a New Class of Weapons," 2017, https://www.rand.org/pubs/research_reports/RR2137.html.

[128] Terri Moon Cronk,"Mattis Sees No Change in Russian Military Capability in Light of Putin's Speech," March, 2018, https://dod.defense.gov/News/Article/Article/1463160/mattis-sees-no-change-in-russian-military-capability-in-light-of-putins-speech/

[129] Aaron Mehta, "Three thoughts on hypersonic weapons from the Pentagon's technology chief," Defense News, July, 2018, https://www.defensenews.com/air/2018/07/16/3-thoughts-on-hypersonic-weapons-from-the-pentagons-technology-chief/.

[130] Tom Demerly, "Russia Test Fires New Kh-47M2 Kinzhal Hypersonic Missile," The Aviationist, https://theaviationist.com/2018/03/12/russia-test-fires-new-kh-47m2-kinzhal-hypersonic-missile/

[131] Mach refers to the speed of sound. The value depends on the gas thermo-physical properties and its density. At 11 km of height, 1 Mach equals 1064 km/hour.

[132] Larry Rubin L. and Stulberg A. "The end of strategic Stability, Nuclear Weapons and the Challenge of Regional Rivalries," Georgetown University Press, 2018.

[133] James M. Acton, "Hypersonic Boost-Glide Weapons,» Science & Global Security 23 (2015), www.tandfonline.com/10.1080/08929882.2015.1087242.

[134] "KH-15," weaponsystems, http://weaponsystems.net/weaponsystem/HH08%20-%20AS-16%20Kickback%20(Kh-15).html

[135] TASS Russian News Agency, "Peresvet combat lasers enter duty with Russia's armed forces," December 5, 2018, url: http://tass.com/defense/1034344.

[136] GlobalSecuity.org, "Peresvet» Combat Laser Complex," July 2018, https://www.globalsecurity.org/military/world/russia/vlk.htm

[137] Ronald O'Rourke, "Navy Shipboard Lasers for Surface, Air, and Missile Defense: Background and Issues for Congress," 2015.

[138] Giri. High-power Electromagnetic Radiators: Nonlethal Weapons and Other Applications. Page 144. Harvard, Cambridge MA. 2004.

[139] Giri. High-power Electromagnetic Radiators: Nonlethal Weapons and Other Applications. Page 145. Harvard, Cambridge MA. 2004.

[140] Giri. High-power Electromagnetic Radiators: Nonlethal Weapons and Other Applications. Page 145. Harvard, Cambridge MA. 2004.

[141] Lewer, Nick. *Introduction*. The Future of Non-Lethal Weapons. Frank Cass. London. 2002.

[142] Giri. High-power Electromagnetic Radiators: Nonlethal Weapons and Other Applications. Page 142. Harvard, Cambridge MA. 2004.

[143] Giri. High-power Electromagnetic Radiators: Nonlethal Weapons and Other Applications. Page 142. Harvard, Cambridge MA. 2004.

[144] Hambling, David. *Maximum pain is aim of new U.S. weapon*. New Scientist. 2 March 2005. <https://www.newscientist.com/article/dn7077-maximum-pain-is-aim-of-new-us-weapon/>

[145] Giri. High-power Electromagnetic Radiators: Nonlethal Weapons and Other Applications. Page 140. Harvard, Cambridge MA. 2004.

[146] Giri. High-power Electromagnetic Radiators: Nonlethal Weapons and Other Applications. Page 139. Harvard, Cambridge MA. 2004.

[147] Giri. High-power Electromagnetic Radiators: Nonlethal Weapons and Other Applications. Page 31. Harvard, Cambridge MA. 2004.

[148] *MH17 Ukraine plane crash: What we know*. BBC News. 28 September, 2016. <http://www.bbc.com/news/world-europe-28357880>

[149] Sun-tzu, translated by Samuel B. Griffith. *The Art of War*, Oxford: Clarendon Press, p. 26.

[150] The "bleeding edge" is a term that originated in computer science to refer to software "that the user is required to risk reductions in stability and productivity in order to use it." The "bleeding edge" is in front of the "cutting edge." A technology may be considered bleeding edge under the following conditions: (1) lack of consensus, such that potential competing mechanisms exist, however, the most successful (usually with respect to market success) technology is highly uncertain. These may include but are not necessarily concepts that challenge Kuhn's "paradigms" of normal science (Thomas S. Kuhn, *The Structure of Scientific Revolutions*, (Third edition, University of Chicago Press, 1996). (2) lack of wide dissemination: organizations are trying to implement a new technology or product of which the overall industry (and its trade publications) are not aware. (3) resistance to change: experts and industry leaders are skeptical or outspokenly averse to a new technology or product but a single or few organizations are pursuing implementation because they are convinced it is technically superior. (See: Kelvin Don Nilsen and Alleen Pace Nilsen, "Literary Metaphors and Other Linguistic Innovations in Computer Language," *English Journal*, vol 84, October 1995, pp 65-71.)

[151] Ben Casselman The Slow Death of American Entrepreneurship, 15 May 2014, https://fivethirtyeight.com/features/the-slow-death-of-american-entrepreneurship/; John Haltiwanger, Ian Hathaway, Javier Miranda, *Declining Business Dynamism in the U.S. High-Technology Sector*, Kauffman Foundation, February 2014, http://www.kauffman.org/~/media/kauffman_org/research%20reports%20and%20covers/2014/02/declining_business_dynamism_in_us_high_tech_sector.pdf

[152] Cassidy R. Sugimoto, Nicolas Robinson-Garcia, Dakota S. Murray, Alfredo Yegros-Yegros, Rodrigo Costas& Vincent Larivière, "Scientists have most impact when they're free to move," *Nature* 550, 29–31 (05 October 2017), https://www.nature.com/news/scientists-have-most-impact-when-they-re-free-to-move-1.22730

[153] William Kerr, "America, don't throw global talent away," *Nature* 563, 445 (2018), https://www.nature.com/articles/d41586-018-07446-2

[154] http://www.pewglobal.org/2013/07/18/chapter-1-attitudes-toward-the-united-states/

[155] Kosal, M. E. U.S. Policies to Reduce the Threat of Chemical Terrorism. In *9/11 + 6 Initiative Foreign Policy Priorities for a Secure America*, The Partnership for a Secure America, May 2008, http://www.psaonline.org/downloads/CHEMICAL%20report%208-28-08.pdf

General Philip Breedlove (U.S.AF, ret.) served as Supreme Allied Commander Europe from 2013 to 2016 and is now a distinguished professor at the Sam Nunn School of International Affairs at the Georgia Institute of Technology. Dr. Margaret Kosal is an associate professor at the Sam Nunn School, where she focuses on technology, strategy, and governance.

Supporting Data

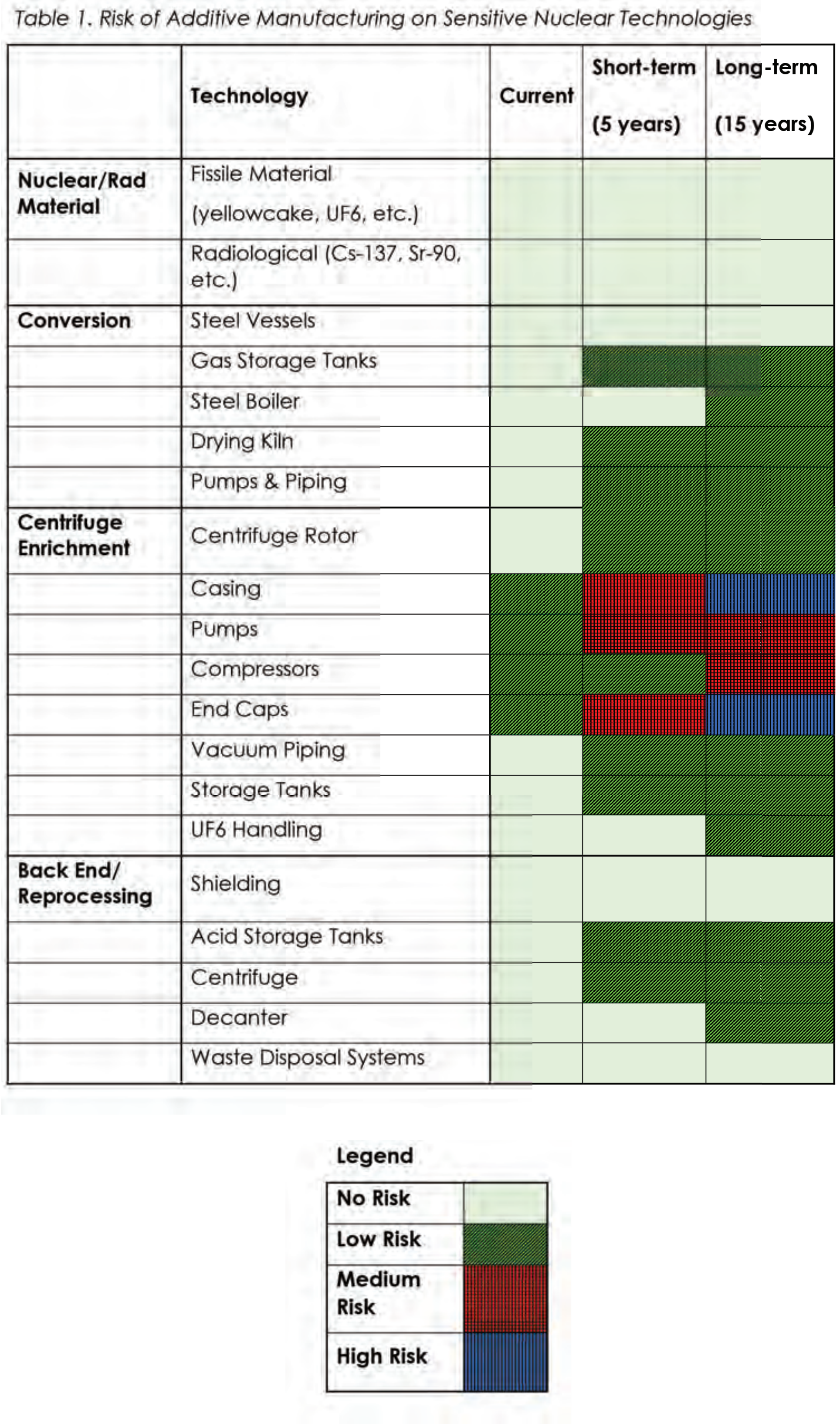


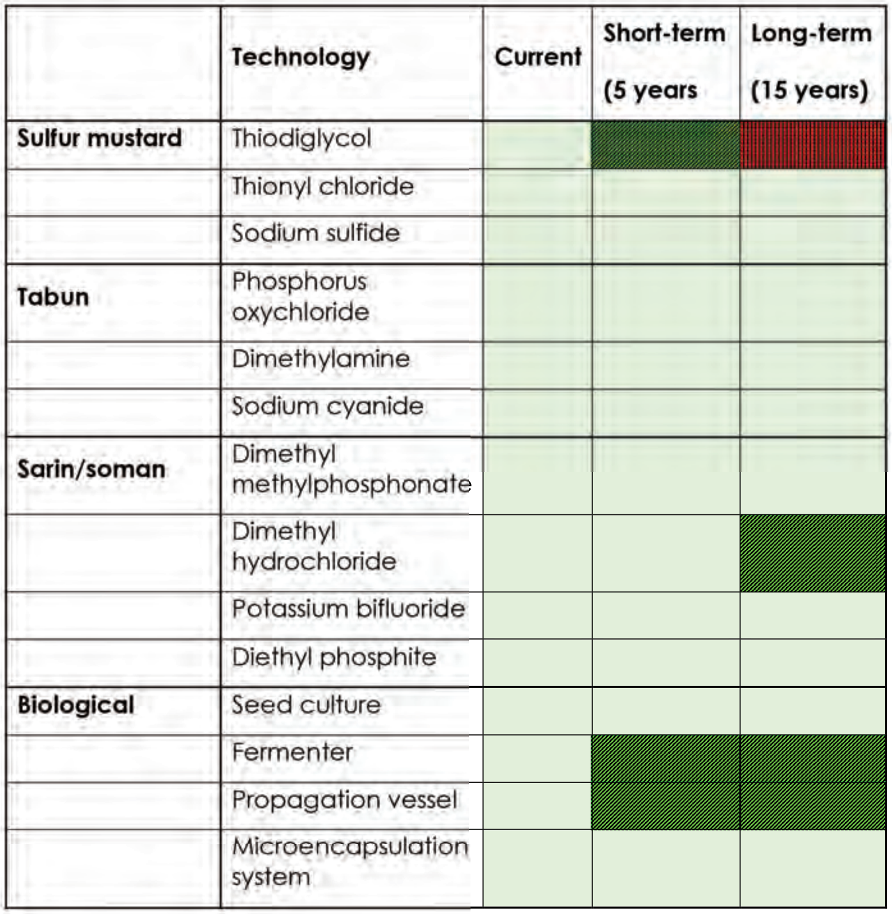
Table 1. Risk of Additive Manufacturing on Sensitive Nuclear Technologies

	Technology	Current	Short-term (5 years)	Long-term (15 years)
Nuclear/Rad Material	Fissile Material (yellowcake, UF6, etc.)	⬜	⬜	⬜
	Radiological (Cs-137, Sr-90, etc.)	⬜	⬜	⬜
Conversion	Steel Vessels	⬜	⬜	⬜
	Gas Storage Tanks	⬜	🟩	🟩
	Steel Boiler	⬜	⬜	🟩
	Drying Kiln	⬜	🟩	🟩
	Pumps & Piping	⬜	🟩	🟩
Centrifuge Enrichment	Centrifuge Rotor	⬜	🟩	🟩
	Casing	🟩	🟥	🟦
	Pumps	🟩	🟥	🟥
	Compressors	🟩	🟩	🟥
	End Caps	🟩	🟥	🟦
	Vacuum Piping	⬜	🟩	🟩
	Storage Tanks	⬜	🟩	🟩
	UF6 Handling	⬜	⬜	🟩
Back End/ Reprocessing	Shielding	⬜	⬜	⬜
	Acid Storage Tanks	⬜	🟩	🟩
	Centrifuge	⬜	🟩	🟩
	Decanter	⬜	⬜	🟩
	Waste Disposal Systems	⬜	⬜	⬜

Legend

No Risk	⬜
Low Risk	🟩
Medium Risk	🟥
High Risk	🟦

Table 2. Risk of Additive Manufacturing on Sensitive Chemical and Biological Material

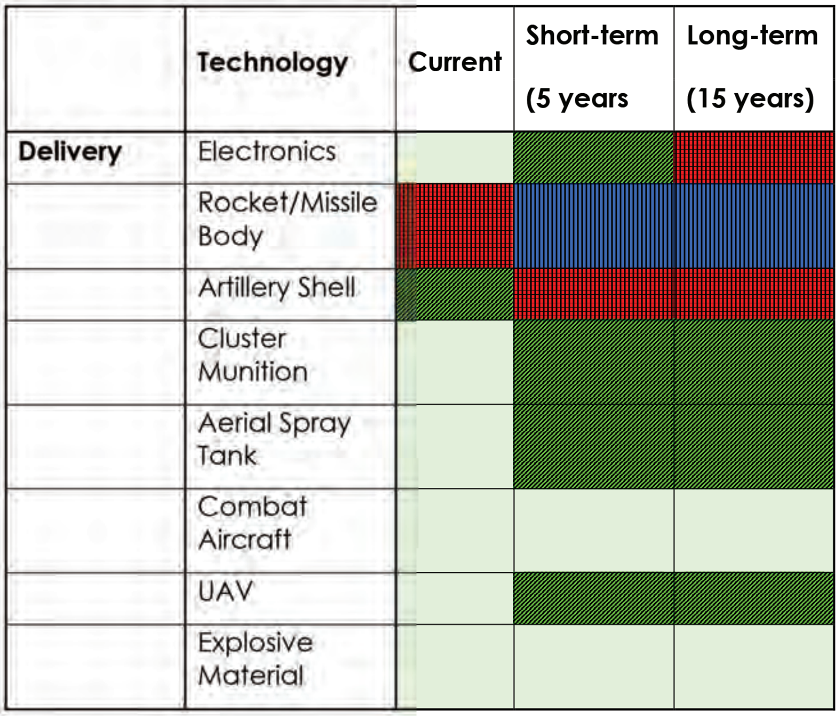


	Technology	Current	Short-term (5 years	Long-term (15 years)
Sulfur mustard	Thiodiglycol	🟩	▨	🟥
	Thionyl chloride	🟩	🟩	🟩
	Sodium sulfide	🟩	🟩	🟩
Tabun	Phosphorus oxychloride	🟩	🟩	🟩
	Dimethylamine	🟩	🟩	🟩
	Sodium cyanide	🟩	🟩	🟩
Sarin/soman	Dimethyl methylphosphonate	🟩	🟩	🟩
	Dimethyl hydrochloride	🟩	🟩	▨
	Potassium bifluoride	🟩	🟩	🟩
	Diethyl phosphite	🟩	🟩	🟩
Biological	Seed culture	🟩	🟩	🟩
	Fermenter	🟩	▨	▨
	Propagation vessel	🟩	▨	▨
	Microencapsulation system	🟩	🟩	🟩

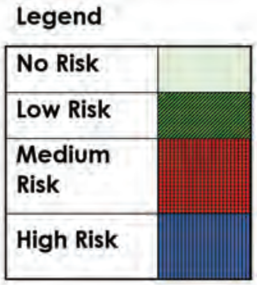
Legend

No Risk	🟩
Low Risk	▨
Medium Risk	🟥
High Risk	🟦

Table 3. Risk of Additive Manufacturing on Weapons Delivery Systems



	Technology	**Current**	**Short-term** **(5 years**	**Long-term** **(15 years)**
Delivery	Electronics	⬜	🟩	🟥
	Rocket/Missile Body	🟥	🟦	🟦
	Artillery Shell	🟩	🟥	🟥
	Cluster Munition	⬜	🟩	🟩
	Aerial Spray Tank	⬜	🟩	🟩
	Combat Aircraft	⬜	⬜	⬜
	UAV	⬜	🟩	🟩
	Explosive Material	⬜	⬜	⬜



Legend

No Risk	⬜
Low Risk	🟩
Medium Risk	🟥
High Risk	🟦

Technology Converges; Non-State Actors Benefit

By T.X. Hammes, National Defense University

The Fourth Industrial Revolution will provide insurgents and terrorists with capabilities that, until very recently, were the preserve of large, powerful, wealthy states. The convergence of new technologies will provide them access to relatively cheap, long-range, autonomous weapons. To define the problem this presents to the United States, this paper will first explore the technologies—powerful small warheads, autonomous drones, task-specific artificial intelligence, and advanced manufacturing—that are providing increased range, numbers, and lethality for dramatically lower cost today. It will close the technology discussion with a brief examination of biotechnology, which has enormous potential as a weapon but, fortunately, remains mostly beyond the reach of non-state actors today.

However, the most important point to remember is that while new technologies will make tactical operations against insurgents much more difficult, U.S. failures against non-state actors have consistently been caused by strategic deficiencies not tactical ones. Therefore, following the discussion of emerging technologies, it will examine how changing political, social, and economic conditions are changing the strategic environment of state versus non-state conflicts. Then, tying the technology to these new strategic conditions, it will suggest ways in which non-state actors will exploit the new technologies and new conditions to defeat states. The paper will close with a discussion of what approaches have worked for the United States in the past and how it may be adapted to the new conditions.

Key Technologies

The starting point of the technology discussion must be the recent history of non-state actors' use of technology. In the 1980s, the author worked with ten different insurgent groups in different regions. Despite U.S. efforts to encourage these groups to use cutting-edge technology, uniformly they refused. Further, if one studies their use of technology, one finds that non-state actors, with the exception of certain drug cartels, primarily use technology that is widely available in their societies. They seemed to do so for two reasons. First, they lacked confidence in cutting-edge technology—and since they were betting lives on it, they were reluctant to use it. They wanted to use technology they were comfortable with and confident in. For instance, when U.S. forces were conducting security operations in Iraq from 2003 to 2008, the Iraqis used common household items such as cell phones, base station phones, and garage door openers to detonate their improvised explosive devices. They did so for good reason. Every neighborhood had a shop that sold and repaired these devices so had the knowledge to modify them for use in weapons. As an added benefit, the use could spread easily across the insurgency.

In contrast, while commercial drones first began flying in the late 1990s, they did not show up in insurgent arsenals until 2014 for surveillance and 2016 for attack.[1] It was not until then that hobbyist and commercial drones were widespread in global society. Even then, ISIS required a focused effort to build and operate them. A special unit kept detailed records of operations to improve their effectiveness.[2] By 2018, insurgent drone use had spread to Afghanistan. And criminal elements have begun to use drones both for surveillance and to disrupt police operations.[3]

While it is a bit comforting to know non-state actors have not been at the leading edge of technology historically, we do have to expect insurgent and terrorist groups to use technology as it becomes widely available in civil society.

With that as a caveat, it's time to look at the new technologies that will present non-state actors with greatly enhanced capabilities in the immediate future. The fourth industrial revolution has already proliferated a series of technological advances that have created a generation of small, smart, and cheap weapons. Progress in small warheads, drones, task-specific artificial intelligence, advanced manufacturing, and cheap space have converged to provide insurgents with capabilities that used to be the preserve of large, technologically-advanced states. This paper will first examine the technologies themselves, then look at how they empower non-state actors.

Small Warheads

While new explosives are increasing the power of warheads, the most effective use of small warheads is to adopt the concept of "bringing the detonator not the explosive." Rather than building a system to deliver a large warhead, this concept uses a small, smart drone to detonate the very large explosive potential present in society such as commercial aircraft, fuel trucks, or fixed facilities with fuel, fertilizer, and other industrial chemical storage sites. This is not a theoretical approach. It has already been used repeatedly. From 2015 through 2017, Russian operatives or Ukrainian separatists used drones to drop simple thermite grenades in a series of attacks on Ukrainian government ammunition dumps that detonated hundreds of thousands of tons of explosives.[4]

A second approach for increasing the destructive power of a small warhead is the use of an explosively shaped penetrator (EFP). An EFP approximately 1 inch in diameter with as little as 1 ounce of high explosive can penetrate up to 1/2 inch of steel.[5] Such a device is small enough to be mounted on a wide variety of small drones to serve as the detonator. It could easily detonate the commercial fuel trucks that have been essential to U.S. operations in Afghanistan and Iraq. It is also powerful enough that if fired into the hood of a motor vehicle it will destroy the engine resulting in a mobility kill. And they are capable of attacking moving vehicles. As early as 2013, hobbyists were using drones with GoPro cameras to film individual trucks and drivers in off-road races.[6] Simply mounting a small EFP next to the lens of the Go-Pro camera would allow the operator to fire the EFP where the camera is pointed. An operator can selective a specific vehicle even in fast moving traffic.

While EFPs have been used widely in Iraq, the insurgents were limited to placing ground IEDs and hoping the target passed over it. Drones allow the attacker to actively hunt selected targets even if they are behind blast walls. It is also possible to create warheads with multiple penetrators[7] and self-forging fins[8] to increase stand-off ranges and lethality.

Advanced Manufacturing

Advanced manufacturing will allow the production of tens of thousands of small, smart, but inexpensive drones. It combines additive manufacturing (aka 3D printing), robots, and artificial intelligence to massively increase the speed and quality of manufacturing. In the last decade, as 3D pioneers mastered various materials and techniques, they began to focus on speed of printing. Of particular importance in small drone production is rapid printing of composite material. In April 2016, Carbon introduced a commercial 3D printer that was 100 times faster than previous printers. In addition to speed, the continuing massive investment in 3D printing has improved both quality and complexity of manufactured products while reducing prices. Prices have dropped to point weekend hobbyists are printing their own drones. A popular website even rates the top 10 3D printed drone kits for sale commercially.[9]

Drones

The dramatic increase in 3D printing speeds has major implications for warfare. In 2014, researchers at the University of Virginia successfully 3D printed a drone in one day. By snapping in place an electric motor, two batteries, and an Android cell phone, they made an autonomous drone with a range of approximately 50 kilometers. It took about 31 hours to print and assemble the drone at a total cost (excluding the printer) of about $800.[10] While it could be controlled by a ground station, the GPS in the phone allowed the drone to fly a specified route autonomously. Such a system is vulnerable to GPS jamming but a number of new approaches are being developed that will allow drones to navigate in GPS denied environments.[11]

Other programs allow a cell phone camera to identify people and objects even under low light conditions.[12] Combining small warheads, GPS-independent navigation, and cell phone target identification can create autonomous, inexpensive drones that can range for dozens of miles, then hunt and engage specific targets. Think of them as IEDs that hunt you.

Long-range air[13] and undersea autonomous drones[14] are also being produced today, and manufacturers are competing hard to reduce the price even as they dramatically increase range and payload. The Aerovel Flexrotor has a range of 1,500 miles, the Defiant Lab DX-3 over 900 miles,[15] and the Volans-I over 500 miles while carrying a 20 pound payload at sustained speeds of 150 miles per hour.[16] While not technically stealthy, the small size of these systems mean they have the radar signature of a small bird.[17] And, like most new technologies, these systems can be greatly improved for relatively little money. Thus naval and air forces will also be at risk from inexpensive, smart, long-range weapons. In particular, fixed facilities like air bases will be vulnerable.

Globally, state militaries are developing very high capability drones. However, this paper will not discuss them since they remain beyond the reach of most insurgent and terrorist organizations—unless a state sponsor chooses to make them available.

Task-Specific Artificial Intelligence

There is a great deal of disagreement over when or even if general artificial intelligence will emerge. While an interesting discussion, it is irrelevant for the purposes of this paper. Much more important is the current state of limited or task-specific artificial intelligence. While the literature normally refers to this type of AI as limited, task-specific is more accurate. It is better than any human at the specific task it is designed to do. Thus in its niche area, task-specific AI creates a distinct advantage for the nation that fields it first.

To create the AI necessary for truly autonomous attack drones, designers had to address two issues—navigation and target identification. Task-specific artificial intelligence has clearly mastered both. The Israeli Harop drone, initially fielded in 2005, uses GPS guidance to arrive in a target area and then shifts to visual, infra-red, and electronic search modes to identify and attack a target.[18]

Striking the target is a separate problem. It requires the autonomous system to identify a specified target and then maneuver through obstacles to strike it. While this is a very challenging issue, commercial firms are already deploying autonomous air taxis and ground vehicles based on a range of ever more effective, precise, and inexpensive sensors which have obvious applications in improving the hunting capability of autonomous drones. In fact, as of January 2019, commercial firms were offering 9 different models of drones that could autonomous follow and film an athlete to include mountain bikers riding trails.[19]

While western states continue to debate whether autonomous drones will be required to maintain a command and control link so the mission can be cancelled or diverted, insurgents and terrorists will not accept that limitation. Doing so would increase the technical complexity of the systems as well as increase the vulnerability to enemy cyber or microwave defenses. Thus non-state actors are likely to treat a drone as a round of ammunition—fire and forget. By employing autonomous drones without a command link, they eliminate the possibility the drone can be defeated by electronic jamming of the command signal.

Current drones still remain vulnerable to GPS jamming. However, commercial drone developers are working to make their autonomous drones GPS independent and hardening them against microwave signals. By shifting from GPS dependent navigation to inertial plus visual navigation, delivery drones will be able to operate in the urban canyons where GPS signals are often blocked. And, if drone deliver systems are to succeed, the drones must also be immune to local high power emissions from airport radars, high power transmission line, and other commercial sources. This will mitigate one of the most promising defenses against autonomous drones—electronic magnetic pulses generated by high-powered microwaves. As commercial drones become hardened to electronic interference, non-state actors will take advantage of that capability.

Cheap Space Capabilities

Given the very long range of new autonomous drones, a third major technical problem is locating the targets precisely. Years ago, Google Maps and Google Earth solved the problem of finding major installations like airfields, ports, and industrial and political facilities for insurgents. If one wants to know where the C-17s and larger commercial aircraft park at Bagram Air Base in Afghanistan, simply look it up on Google Maps. Shift to satellite mode and you have sufficient resolution to direct a smart drone to within a couple hundred feet of the target. Given Google Maps' global coverage, it provides a first rate intelligence source for anyone with an internet connection. Admittedly these images are dated, but it is a pretty safe assumption the big airplanes still park in the same place and thus a drone with visual target identification could fly to the parking apron and then select a target.

More recently, current imagery has become available to anyone with an internet connection and a credit card. Over the last two decades, the development of cube satellites and the infrastructure to launch them cheaply in large numbers has made space imagery commercially available.[20] Planet, a private company, uses its cube satellite network to take sub-meter resolution imagery of the entire planet *daily* and it sells these images on line.[21] Planet can provide images based on visual or infrared cameras as well as synthetic aperture radar. Apple now provides the SpyMeSat "the only mobile app to offer on-demand access to the latest commercial high resolution satellite imagery, and with the release of v3.1, the only mobile app offering users the ability to task high resolution commercial imaging satellites."[22] The bottom line is that multiple companies now or will soon offer near real time imagery of anywhere on the planet. The days of hiding military movement on the surface are clearly drawing to a close.

Biotechnology

Synthetic biology and rapid advances in gene editing have truly frightening potential. Therefore, while the impact of bio-technology in state versus non-state conflicts is a bit farther out, readers need to understand it has by far the greatest destructive potential. Fortunately, it is very unlikely that non-state actors have the necessary skills and resources to use these advanced tools to create biological weapons. As noted earlier, non-state actors have rarely used cutting-edge technology. Thus any biological attack they generate is much more likely to use commercially available products. For decades, we have speculated that a terror cell could conduct a devastating economic attack on the United States by introducing hoof and mouth disease or mad cow disease into our livestock industry. By infecting an unknown number of animals and then reporting their infection to media outlets, a terror group could cause major economic damage by attacking the U.S. cattle industry. In 2017, it generated almost $90 billion in meat and milk products.[23] Yet, to date, the biological terror attacks in the United States have been very minor such as the 1984

Rajaneeshee poisoning of salad bars, the 2001 Amerithrax attacks on Capitol Hill, and the ricin letters mailed in 2003 and 2004.

While bio-weapons have the most potential, the difficult in producing them has so far prevented non-state actors from using them. However, states must carefully monitor progress in this area. Because while states will hesitate to use such a weapon due to potential infection of its own population as well as massive retaliation, nihilistic terrorist organizations are probably the most likely people to consider losing a contagious disease on the planet.

This brief examination of how non-state actors can exploit new technologies indicates the depth of the tactical problem. However, to understand the strategic problem we must examine the emerging strategic conditions that will govern state versus non-state conflicts.

Drivers of Insurgency

"Military institutions and the manner in which they employ violence depended on the economic, social and political conditions of their respective states."[24]

Even as technology is providing weapons that exploit current western vulnerabilities, the fact remains that economic, social, and political conditions of the various entities in the conflict will determine how the technology is employed. Emerging technologies will challenge every aspect of the current U.S. operational approach to counterinsurgency. An even greater challenge is the fact that changes in the primary political driver of insurgency will make U.S. counterinsurgency doctrine obsolete.

It is essential to understand that the primary cause driving post-World War II insurgencies have evolved. The initial major driver—anti-colonialism—has obviously passed. Colonial powers were driven out. Unfortunately, their withdrawals led directly to the second major driver of insurgencies—conflicts over who would rule the state the colonists established and left behind. The National Union for the Total Independence of Angola (UNITA)'s long war with the Popular Movement for the Liberation of Angola (MPLA) over who would rule Angola is a clear example of this motivation. Despite its ethnic and tribal aspects as well as its 20-year duration, the conflict did not change the territorial borders of Angola.

Now a third driver is gaining prominence—the desire to change the old colonial borders. The colonial borders were drawn without any consideration of the historical ethnic, cultural, or religious networks on the ground. Today, we are seeing an increase in conflicts in regions where the colonial borders artificially divided much older cultures. The Balouch of Afghanistan, Pakistan, and Iran are prime examples. Their society was divided for the convenience of the British colonial government. This has left them as ignored and often persecuted minorities in each of the three existing countries. In response, they have conducted a decades long insurgency in an attempt to establish a homeland. They join the Kurds of the Middle East in struggling against the colonial boundaries. The intra-state conflicts across the Sahel between Arab northern societies and southern African ones also illustrate the failure of colonial powers to create national identities. At the same time, sub-national movements are redefining borders in other areas. The peoples of the old Yugoslavia, Sudan, and Somalia are still working through the process.

The third driver means insurgencies are increasingly transnational, trans-dimensional coalitions of the willing and opportunists. And they will be long. Each aspect creates significant problems for the United States.

Third driver efforts to redraw political boundaries to align with social boundaries means most insurgencies will be transnational. This very fact stymies U.S. counterinsurgency doctrine which is based on working with the host nation. Afghanistan illustrates the problem. The insurgency is primarily Pashtun yet more Pashtuns live in Pakistan than Afghanistan. So there are really two host nations. Further complicating the problem is the fact the two host nations' strategic interests do align. Pakistan feels it must maintain relations with the Taliban as a strategic hedge against India. Yet the Afghan government cannot accept continued Pakistani support for its primary enemy. The United States and its coalition partners have been unable to resolve this fundamental difference of strategic outlooks.

Today insurgencies are also trans-dimensional in that they operate in both the real and cyber world. Driven by necessity, many non-state actors have learned to use the internet both to communicate and recruit. Because boundaries are about identities, it is easier to use social media to involve ethnic diasporas. We have seen the impact of this in recruiting for the conflict in Syria as well as the continuing struggle in Somalia.

In addition, identity-based insurgencies reflect the societies they live in. Given the non-hierarchical nature of many post-colonial societies, they have tended to be coalitions rather than hierarchies. The Afghans, Kurds, Iraqis, Chechens, and Syrians were/are not unified insurgencies but rather coalitions of the willing and the opportunistic. This vastly complicates the counterinsurgent's task because there is no single political entity to either defeat or negotiate with.

Finally, identity-based insurgencies are likely to be very long. The counterinsurgent is not simply trying to build a functioning state to run an existing nation. He is trying to create a nation from a variety of other identities. In Europe and Asia, it took between 400 and 1,000 years to create nations with a common identity. Unfortunately, it also involved a great deal of warfare and often ethnic cleansing. Thus, we should anticipate identity-based insurgencies will be long—think decades not years.

The different drivers have dramatically changed the character of the insurgencies, their organizations, and their approaches to gaining power. But it has not changed the fact they will use force to achieve their goals.

Insurgent Strategy

While a number of insurgents have provided theories of insurgency (Mao, Che, Giap, et.al), there is no general insurgent strategy. However, there is a practical approach that has often worked to convince outside powers to quit fighting and go home. Successful insurgencies have focused on wearing down the political will of the outside power via a campaign of attrition. In the past, the attrition has been limited primarily to attacking the outsiders that have entered the insurgent's country. As will be discussed below, today's technology may open entirely new paths for the insurgents to attack the will of outside powers. Then, as always, the insurgents will have to win the internal civil war against the host nation government. Unfortunately, new technologies will provide new tools for that fight too.

Insurgent Tactical Options Created by 4IR Technologies

With insurgent strategy focused on destroying the will of outside policymakers, insurgents have adopted tactics to maximize outside casualties while "proving" the government is making little or no progress in defeating them. They do not have to seize territory but only visibly continue the fight to prove the government is not succeeding. In the past, equipment limitations meant insurgents were usually limited to direct attacks on counterinsurgent forces and the population in country. And, they often fought at a range and firepower disadvantage.

New technology is changing that. The arrival of commercial drones means insurgents can launch attacks from outside the range of most government surveillance and weapons systems. Unfortunately, current U.S. approaches to fighting insurgents are extremely vulnerable to this type of attack. U.S. forces travel into a theater via large aircraft and then operate from easily identified fortified bases, and move about in distinctive vehicles. In the last 18 years, both Arab and Afghan insurgents focused their attacks on the bases and communications links between them using IEDs and ambushes. They also constantly refined their suicide attacks against fixed positions and public gatherings. While coalition forces developed more effective tactics, techniques, and procedures to defend against this type of attack, doing so required the dedication of enormous resources and severely restricted coalition operations. Through decades of effort, the United States has developed very effective defenses against ground attack by non-state actors. Physical barriers backed by armed personnel who are alerted by extensive surveillance systems have prevents hundreds of attacks from reaching the vulnerable interiors of U.S. facilities. Despite these efforts, coalition forces have only significantly reduced the number of attacks when the mass of the population shifted allegiance to the government

These attacks became less of a problem with the withdrawal of major combat forces from Iraq and Afghanistan. Since then U.S. involvement has focused on advising and providing fire support. The majority of U.S. forces operate from fortified bases. Those that move off base do so in armored vehicles or by air. The combination has dramatically reduced U.S. casualties. Since 2015, more service people have died in peacetime training than combat.[25]

However, each node within the U.S. system, whether U.S. forces are actively fighting the insurgents or are in an advisory role, is vulnerable to attack by autonomous drones. Airfields are the most vulnerable. The very large perimeter and vulnerability of key elements of the system from radars to fuel farms to the aircraft themselves will make these a prime target for insurgent or terrorist attacks. Using Google Maps, insurgents can see the entire layout of airfields that U.S. forces use. Shifting to the satellite image, one can locate the parking apron for C-17s and other large aircraft at Bagram Airfield, Afghanistan. Clearly if a C-17 or large commercial aircraft is damaged or destroyed on the ground, the United States will discontinue airlift into the attacked airfield—and perhaps all airfields in the theater until the threat can be addressed.

Unfortunately, neither the United States nor any other nation has created truly effective defenses against drones. And insurgents recognize the value of attacking aircraft on the ground. While the Russians claim to have defeated all 23 drone attacks against their main air base in Syria,[26] other reports show images of damaged Russian aircraft.[27] Further, it is essential to note most of the Russian success came from using electronic warfare to defeat the drones' very crude control systems or jam the signal from the pilot. As noted, autonomous drones do not have a link to a pilot and can be hardened against high energy microwaves. Soon they will not be susceptible to GPS jamming either.

Another major component of U.S. counterinsurgency operations are fixed outposts. While much smaller than airfields, they are also very numerous. They range from major support facilities with stores of fuel, lubricants, and ammunition to individual platoon outposts and police checkpoints. How can the government protect the thousands of military, police, and government outposts across a nation from drone attack? Consolidating bases would reduce the problem but also dramatically curtail the contact between the population and the government. And of course the capability to direct air attacks means the use of public meetings or "shuras," a key element of U.S. counterinsurgency doctrine, becomes a much more difficult and hazardous problem. This threat can further reduce the critical contact between the government and the people.

Perhaps the most difficult to protect from cheap, fast drones are the ground convoys and patrols that are an essential part of counterinsurgency operations. Insurgents in both Iraq and Afghanistan have severely restricted ground movement of coalition forces through the use of improvised explosive devices. Despite enormous effort by coalition forces hunting IEDs and the networks that produce them, government forces have been unable to neutralize this threat. The addition of fast, small drones will complicate the problem immensely. If a cheap commercial drone can autonomously identify and track a runner in motion, it can identify and fly into a vehicle or a patrol. The IEDs will now be actively hunting both moving and stationary government assets.

As early as January 2017, ISIS was conducting at least one drone mission a day over coalition forces.[28] To increase the impact of their attacks, they released numerous videos of their drones attacking coalition forces.[29] One even showed a complex attack with a drone dispersing the personnel at a checkpoint to clear the way for a suicide car bomb attack.[30] Clearly the sophistication of the attacks will continue to improve. And as 3D printing of drones becomes more widespread, we should expect to see a significant increase in the number of drones employed.

In addition, very long range drones like the Flexrotor, Volans-I, and DX-3 will become widely available. Well-funded insurgent or terrorists groups will inevitably arm one or more. They can then reach out of theater to threaten U.S. forces in transit. Drawing a 1,500 mile range ring around ISIS or Taliban territory gives an idea of how deeply these systems can strike into America's logistics pipeline.

A more sophisticated group could blackmail other nations to refuse U.S. transit rights. Recent events at Heathrow and Gatwick demonstrated the difficulty of preventing drones from entering airspace around an airfield. And a small drone can easily carry enough explosives to damage a 777 or an A380 parked at a gate on a major airfield—with accurate placement it could ignite a secondary explosion from the fuel on board. Thus an insurgent or terror group could offer a state like Germany or Kuwait a choice: terminate U.S. support flights passing through your nations or face attacks on your air transportation industry. A single successful attack will result in billions worth of economic damage if the nation refuses the insurgent demands.

In short, the emergence of large numbers of autonomous armed drones will require the United States to rethink its entire concept of counterinsurgency operations.

Terrorist Options

If terrorists adapt drones, they effectively neutralize 95% of all anti-terror physical barriers. The last few decades have taught security forces that layered protection against a ground attack is essential. Governments, businesses, and even private individuals have invested in walls, barriers, vehicle mazes, ditches, barbed wire, and other physical obstacles all backed up by armed guards. For the most part, standoff distance and defense in depth have prevented attacks against fixed facilities.

Fortunately, today's commercial drones carry relatively small payloads so will not cause great damage by themselves. Unfortunately, precisely delivered small payloads can be used in a couple of creative ways. First, it can serve as a detonator for the explosive power that is present in any modern society—fuel depots, fertilizer storage facilities, key elements of the power grid, and chemical plants. In 1947, the *SS Grandcamp* caught fire which resulted in the detonation of 2,200 tons (a 2 kiloton equivalent) of ammonium nitrate fertilizer that killed over 500 people and flattened the Port of Texas City.[31] The 1984 Union Carbide disaster in Bhopal, India released tons of methyl isocyanate that resulted in thousands dead and hundreds of thousands injured.[32] These two accidents clearly demonstrate the massive level of destructive power embedded in the commercial sector. New technologies will provide terrorists with the ability to precisely deliver the detonator to set off the explosive energy spread across modern society.

For high visibility attacks, terrorist have consistently attacked aircraft. Today's airport security has made that very difficult. However, a small drone bypasses virtually all current airport defenses and can deliver high explosive or incendiary devices directly to an aircraft parked at a gate. For a terrorist group intent on doing maximum economic damage to the global economy, simultaneous attacks on key international air hubs will fill the bill. By selecting airports in nations that lack global reach for counterattacking, the terrorists can also reduce the risk to themselves. Using 5-10 small drones at each target airfield, terrorists can be relatively certain of hitting at least one target. Of course, they would video the attack and release the video on line immediately. The financial impact of striking multiple key nodes in the global air system will be enormous. Today air cargo accounts for 35% of global trade by value—not including the value of transporting passengers.[33] If multiple nodes are struck at once, air operations will have to cease while risk assessment and mitigation are conducted. Given the current state of defense against drones, it is likely the shutdown will endure for weeks if not months as governments try to solve this exceptionally difficult security issue.

A second approach is to use precision to strike just key government officials or uniformed security forces. This has three effects. It shows the people the terrorists are only fighting the government and not the people; it separates the security forces from the people as they build barriers between themselves and the populations; and it shows the government cannot even protect itself much less the population. And of course, precision drones can be used for high profile attacks or assassinations. Drones have already been flown very close to two national leaders—German Chancellor Angela Merkel and Venezuelan President Nicolas Maduro.

Criminal Organizations

While not strictly speaking a form of insurgency, crime has also become a major driver of instability in many nations. Criminal organizations across the globe are challenging governments for control of territory. They emerge in numerous forms from gangs to drug cartels to transnational criminal networks that deal in commodities from guns to drugs to people. With the exception of first-generation street gangs, these criminal organizations have a common motivation—profit.[34] While some commentators dismiss this as a law enforcement problem, criminal organizations have demonstrated the ability both to ally with insurgents (Colombia) or effectively seize and rule territory within a state (Mexico). These cases demonstrate how criminals can impact the security of the United States.

As commercial drone usage expands, criminals have been quick to see the possibilities. In 2017, Australian police arrested members of a drug gang that were using drones to warn them if police were in the area.[35] In May 2018, reports emerged that criminals had used a swarm of drones to disrupt an FBI hostage rescue operation by repeatedly buzzing the FBI surveillance team.[36] Numerous drones have been intercepted smuggling drugs, phones, or money over prison walls as well as smuggling drugs across international boundaries. As drone capabilities increase, we can expect to see increased usage by criminals with a focus on smuggling, surveillance, and intelligence operations. And we have to assume criminals will soon be using suicide drones for attacks on opponents.

How Can the United States Respond?

In short, the drivers of insurgency, terror, and criminal activity are not going away. Their widespread distribution means it is inevitable these conflicts will destabilize important allies or impinge on world energy supplies. The United States may also have to respond when a party or parties to a conflict provides sanctuaries for terrorists targeting the United States or its allies. To do so, we have to develop a strategic approach to each separate problem—insurgency, terror, and crime.

Unfortunately, the very phrases "counterinsurgency or counterterror strategy," confuse methods or ways of fighting with a complete strategy. Neither is a strategy. They are merely one approach in a range of possible ways in the ends, ways, and means formulation of strategy.

Population-centric counterinsurgency, as documented in *FM 3-24 Counterinsurgency*, is only one possible approach to such a campaign. A disturbingly large portion of the discussion within the United States government simply accepts *FM 3-24's* recommended best practices and believes that, if applied as package, they create a strategy. Yet by nature, best practices in counterinsurgency are essentially tactical or, at the most, operational level efforts.

In fact, there is no general counterinsurgency or counterterror strategy just as there is no anti-submarine or anti-aircraft strategy. One doesn't develop a strategy against an operational technique. Each conflict requires the development of a case-specific strategy that includes assumptions, coherent ends-ways-means, priorities, sequencing of events, and a theory of victory. And it must be flexible enough to respond to the changes that are an inevitable part of any conflict.

Rather than unquestioningly accepting that "counterinsurgency or counterterror strategy" is the correct solution to a conflict, planners must start by first understanding the specific conflict. Since it will be impossible to know everything necessary to develop a strategy, they must next think through and clearly state their assumptions about that specific conflict. With this level of understanding, they will be ready to start the difficult process of developing coherent ends, ways, and means, prioritizing and sequencing their actions, and developing a theory of victory. Only then will they have a strategy that is appropriate for the actual conflict.

What Has Worked for the United States as an Expeditionary Power?

In considering the various counterinsurgency approaches, the most important question for the United States is what works best for an expeditionary power. When discussing the future of U.S. counterinsurgency, it is absolutely essential to differentiate between those approaches that worked for domestic campaigns and those that work for expeditionary campaigns. Unfortunately, *FM 3-24 Counterinsurgency* drew most of its best practices from the domestic counterinsurgency efforts of the British in Malaya and North Ireland and the French in Algeria. In all three cases, the counterinsurgent was also the government. Thus, they could make the government legitimate by removing any person or organization that was hurting that legitimacy.

It is much more difficult for an outside power to force the host country to make the necessary political changes. As the United States experienced in Vietnam, Iraq, and Afghanistan and the Soviets in Afghanistan, an outside power cannot force the government to be legitimate. Even removing illegitimate leaders and replacing them with those picked by the expeditionary power failed for the United States in Vietnam and for the Soviets in Afghanistan.

That said the United States has been successful at expeditionary counterinsurgency. U.S. efforts to assist the Philippines in 1950s and again since 2001, Thailand from the 1950s to the 1970s, El Salvador in the 1980s, and Colombia against its insurgents in the 1990s and 2000s have all been successful. In each case, the United States used an indirect approach rather than a direct approach. The indirect approach meant that U.S. personnel provided advice and support to host nation forces as those nations fought. While this support at times even included tactical leadership, the focus was always on assisting the host nation and not on U.S. elements engaging the enemy. In addition, these efforts were kept relatively small. This had two major benefits. First, it kept the U.S. presence from distorting the local political and economic reality too badly. Second, it prevented impatient Americans from attempting to do the job themselves because they simply lacked the resources to do so.

Based on our historical record, America should only provide advice and assistance to the host nation or nations in a counterinsurgency campaign. As insurgents employ larger numbers of more effective, longer range precision weapons, the United States will have to modify its approach to even this mission. It will want to minimize the presence of U.S. government personnel in the country and adopt a more austere, expeditionary footprint. In particular, while continuing to pursue technological approaches to defeating drones, it must fall back on ancient methods. Overhead protection—even something as simple as dirt—can defeat the vast majority of drones. All U.S. government facilities will require overhead protection of key nodes or sources of explosive energy like fuel tanks, large vehicles, etc. The second approach is to strive to blend into the population. Rather than moving about in high profile armored vehicles, whether military or armored Chevy Suburbans, U.S. personnel should travel in local vehicles without ostentatious security.

A further major benefit of keeping any supporting effort small is that it extends the timeline. By remaining small, the effort remains below the interest level of the vast majority of Americans and thus can be sustained for the very long timelines of a nation building effort. Just as important, if despite our assistance, the government fails to reform and achieve popular support, the United States needs to admit it cannot fix another country and withdraw. By keeping the effort small, it allows us to do so without a major loss of international credibility.

Does the United States Need a Counterinsurgency Capability?

The high cost and lack of success in Iraq and Afghanistan means hostility to counterinsurgency as a concept is rising. Yet, the capability has enduring relevance. Nor is it only relevant in the event of some distant future conflict. It is an essential element of national security today. One of the critical issues facing today's Pentagon is designing and building the appropriate force structure in the resource constrained, post-Afghanistan period. The United States must balance the risk of not being prepared in some mission areas against the ongoing cost of maintaining readiness across the spectrum of conflict. If the counterinsurgency skeptics prevail, then the United States may choose to severely reduce or eliminate the capabilities necessary for fighting an insurgency. In short, the Pentagon could choose the same route that left the nation intellectually unprepared for the conflicts in Iraq and Afghanistan. It failed to anticipate the insurgencies that were almost inevitable and when it did accept the insurgencies were happening, responded very slowly.

Rather than arguing about the effectiveness or ineffectiveness of a non-existent strategy, we need to be discussing if the United States needs to maintain counterinsurgency capabilities in its national security tool kit? If so, what should such capabilities focus on? Is there an approach or approaches that have been successful for expeditionary forces in insurgencies? How do we modify them to the new capabilities that insurgents are already using? Answers to these questions are an essential part of answering the larger question concerning future U.S. force structure.

Counterterrorism Strategy

As U.S. strategic documents from the National Security Strategy to the U.S. Director of National Intelligence assessments have noted, terrorist groups remain a threat to the United States. However, the sheer magnitude of the problem prohibits the United States from "fixing" the dozens of countries that are both the source and target of terror groups. There is an emerging understanding that, like many wicked problems, terror cannot be fixed but only managed. Thus the United States continues to conduct operations globally to reduce terrorists' capabilities to strike. Sometimes referred to as "mowing the grass" this ongoing campaign recognizes it is only an attempt to manage a problem beyond our capability to solve.

Unfortunately, the capabilities emerging from the fourth industrial revolution make it inevitable that terrorists will be able to conduct more effective attacks on U.S. facilities and personnel overseas and even in the United States.

Thus resilience will become a much greater part of U.S. counterterror approach. The American people must understand that some attacks will get through and that the United States will NOT launch a multi-decade, multi-trillion dollar effort to fix the country that was the source of the attacks. Rather the United States will continue to work to preempt attacks and improve its resilience but will have to accept that terrorists will occasionally succeed.

Dealing with Crime

Profit seeking criminals will be happy to exploit new technology but will use it mostly to avoid contact with the police. Contact, potential conflict, and confinement greatly increase the cost of doing business. Dealing with these groups should be based on police methods—adapted as necessary to deal with increasing criminal capability. Unfortunately, this is likely to result in further movement of policing to a paramilitary basis which historically has not boded well for the people of the nation.

In contrast, those criminals who choose to carve territory out of a state to prevent state interference in their business have really moved into the realm of insurgency. They are seizing political control of a region. Dealing with these groups will require more of a counterinsurgency concept like that described above.

Conclusion

The converging technologies of the fourth industrial revolution are shifting the military balance between states and non-state actors in favor of the non-state actors. Insurgents, terrorists, and criminals now have access to capabilities formerly reserved for major powers. The United States will have to adapt accordingly. But the most important point to remember is that our failures since World War II have not been the result of an inability to solve tactical problems but rather the consistent failure to match U.S. strategy to the particular situation. Therefore the critical piece is to truly understand the problem and adopt a strategy that solves the problem confronting the United States. Then we can adapt at the tactical and technical levels to deal with the new problems presented by emerging technology.

[1] Kate Conger, "How consumer drones wind up in the hands of ISIS fighters," *TechCrunch,* October 13, 2016, https://techcrunch.com/2016/10/13/how-consumer-drones-wind-up-in-the-hands-of-isis-fighters/.

[2] Eric Schmitt, "Papers Offer a Peek at ISIS' Drones, Lethal and Largely Off-the-Shelf," *New York Times,* January 31, 2017, https://www.nytimes.com/2017/01/31/world/middleeast/isis-drone-documents.html.

[3] Jonathan Vanian, "Criminals Used a Fleet of Drones to Disrupt an FBI Hostage Operation," *Fortune,* May 4, 2018, http://fortune.com/go/tech/drone-fbi-hostage-criminals/.

[4] Kyle Mizokami, "Another Ukrainian Ammo Dump Goes Up in Massive Explosion," *Popular Mechanics,* September 27, 2017, https://www.popularmechanics.com/military/weapons/news/a28412/ukrainian-ammo-dump-explosion/.

[5] "EFP Charge Demonstration Video," ISSEE, https://www.youtube.com/watch?v=G0ZOPFiuOL8.

[6] XP2 Quadcopter Off Road Racing Demo Reel - Aerial Video and Photography, *YouTube,* July 3, 2013, https://www.youtube.com/watch?feature=player_embedded&v=QRrSriR5b6s.

[7] Richard Fong, et.al., "Multiple Explosively Formed Penetrator (MEFP) Warhead Technology Development," 2004, www.dtic.mil/get-tr-doc/pdf?AD=ADA432897.

[8] Jian-qing Liu, et.al., "Formation of explosively formed penetrator with fins and its flight characteristics," *Defence Technology,* June 2014, Vol 10, Iss 2, 119-123, https://www.sciencedirect.com/science/article/pii/S2214914714000348.

[9] "Top 10 3D printed drones," *3Dnatives,* December 10, 2018, https://www.3dnatives.com/en/top-3d-printed-drones-101220185/.

[10] Jordan Golson, "A Military-Grade Drone That Can Be Printed Anywhere," *Wired,* Sep 16, 2014, http://www.wired.com/2014/09/military-grade-drone-can-printed-anywhere.

[11] Riley Bauer, Shannon Nollet, and Dr. Saad Biaz, "A Novel Approach to Non-GPS Navigation Using Infrasound. Technical Paper #CSEE14-03," September 11, 2014, www.eng.auburn.edu/files/acad_depts/csse/csse_technical_reports/csse14-03.pdf.

[12] Hillary Grigonis, "Google designed an object-recognition program that won't need the internet," *Digital Trends,* June 15, 2017, https://www.digitaltrends.com/mobile/google-mobilenets-open-source/.

[13] "US Government Makes Aerovel's Flexrotor ITAR-Free," Aerovel News Release, November 24, 2014, http://aerovel.com/aerovel-flexrotor-itar-free/.

[14] Mark Thompson, "The Navy's Amazing Ocean-Powered Underwater Drone," *Time,* December 22, 2013, http://swampland.time.com/2013/12/22/navy-underwater-drone/.

[15] "Flexrotor Specification," http://aerovel.com/flexrotor/ and "Defiant Labs Launches Next Gen Drone: DX-3," Defiant Lab Press release, February 10, 2017, https://news.usaonline.us/press-releases/Defiant-Labs-Launches-Next-Gen-Drone-DX-3-86383.

[16] Lora Kolodny and Darren Weaver, "These drones can haul a 20-pound load for 500 miles and land on a moving target," CNBC, May 26, 2018, https://www.cnbc.com/2018/05/26/volans-i-drones-can-haul-cargo-for-500-miles-and-land-on-a-moving-ship.html.

[17] Tyler Rogoway, "Meet Israel's 'Suicide Squad' of Self-Sacrificing Drones," *The Warzone,* August 8, 2016, http://www.thedrive.com/the-war-zone/4760/meet-israels-suicide-squad-of-self-sacrificing-drones.

[18] "Harop Loitering Munitions UCAV System," *Air Force Technology,* www.airforce-technology.com/projects/haroploiteringmuniti/.

[19] Jesse Wong, "9 Best Drones That Follow You [Crystal Clear Video] 2019," *Drone Guru,* January 11, 2019, http://www.droneguru.net/8-best-drones-that-follow-you-follow-drones/.

[20] "What are small sats and cube sats?" NASA, February 26, 2015, https://www.nasa.gov/content/what-are-smallsats-and-cubesats.

[21] Nathan Hurst, "How Daily Images of the Entire Earth Will Change the Way We Look At It," *Smithsonian.com,* March 13, 2017, http://www.smithsonianmag.com/innovation/how-daily-images-entire-earth-will-change-way-we-look-it-180962467/#J24AmE8xz2EVa3j8.99.

[22] SpyMeSat, https://spymesat.com/.

[23] "Overview of U.S. Livestock, Poultry, and Aquaculture Production in 2017," U.S. Department of Agriculture, https://www.aphis.usda.gov/animal_health/nahms/downloads/Demographics2017.pdf.

[24] Carl von Clausewitz, *On War,* Edited and translated by Michael Howard and Peter Paret, Princeton University Press, Princeton, NJ, 1976, 6.

[25] Erika I. Ritchie, "Training Kills More Troops Than War. Here's What's Being Done About It," *Military.com,* May 14, 2018, https://www.military.com/daily-news/2018/05/14/training-kills-more-troops-war-heres-whats-being-done-about-it.html.

[26] "Rise in drone attacks on Russian airbase in Syria: Monitor," *France24,* August 24, 2018, https://www.france24.com/en/20180824-rise-drone-attacks-russian-airbase-syria-monitor.

[27] Tom Demerly, "Defining Asymmetrical Warfare: Extremists Use Retail Drones to Attack Russian Air Base in Syria," *The Aviationist,* January 8, 2018, https://theaviationist.com/2018/01/08/defining-asymmetrical-warfare-extremists-use-retail-drones-to-attack-russian-air-base-in-syria/.

[28] Ben Watson, "The Drones of ISIS," *DefenseOne,* January 12, 2017, https://www.defenseone.com/technology/2017/01/drones-isis/134542/.

[29] ISIS drone attack videos, *YouTube,* https://www.youtube.com/results?search_query=isis+drone+attack+video.

[30] "ISIS' 'Industrial Revolution of Terrorism'", June 2, 2017, https://www.youtube.com/watch?v=0vY7i_eR06M.

[31] "1947 Texas City Disaster," http://www.texascity-library.org/disaster/first.php.

[32] "Bhopal disaster," *Encyclopaedia Britannica,* January 17, 2019, https://www.britannica.com/event/Bhopal-disaster.

[33] "Air Cargo Matters," *IATA,* https://www.iata.org/whatwedo/cargo/sustainability/Pages/benefits.aspx.

[34] John P. Sullivan and Robert J. Bunker, "Drug Cartels, Street Gangs, and Warlords," *Small Wars and Insurgencies,* March 17, 2008, http://www.academia.edu/36483305/Drug_Cartels_Street_Gangs_and_Warlords.

[35] Ray Downs, "Australian drug gang suspected of using drone to monitor police," *UPI,* June 30, 2017, https://www.upi.com/Top_News/World-News/2017/06/30/Australian-drug-gang-suspected-of-using-drone-to-monitor-police/2911498801791/.

[36] Jason Murdock, "'Drone Swarm' Used by Criminals to Disrupt an FBI Hostage Rescue Operation," *Newsweek,* May 4, 2018, https://www.newsweek.com/drone-swarm-used-criminals-disrupt-fbi-hostage-rescue-operation-910431.

T.X. Hammes is a distinguished research fellow in the Institute for National Strategic Studies at the National Defense University. He served for 30 years in the United States Marine Corps.

Information: The New Pacific Coin of the Realm

By Gary Roughead, *The Hoover Institution, and* **Emelia Spencer Probasco** *and*
Ralph Semmel*, Johns Hopkins Applied Physics Laboratory*

> *I hope that now, after facing for the second time in a generation this great danger, we shall be wise enough and sensitive enough to our duties as citizens never, never to forget the causes of that danger and keep our defense preparations in motion.*
>
> — Dr. Isaiah Bowman, President the Johns Hopkins University, May 3, 1946

Introduction

History informs and rhymes, and the admonition of Isaiah Bowman is as valid today as it was in 1946. A participant in the World War I peace conference in Paris and the president of the Johns Hopkins University, whose Applied Physics Laboratory produced breakthrough innovations during World War II and the Cold War (and today), Bowman understood international challenges and appreciated the role of technology in defining national power. He also understood that it is not one sector or particular endeavor that underpins national security—it is the collective responsibility of society.

Technical Realities

There is a special and increasingly intoxicating allure in the promise of new technologies for national security. The appeal is natural given that technology has always shaped the nature of war—whether the longbow, the airplane, radar, or nuclear weapons. In that context, it is easy and common today to focus on particular technologies that may change the nature of future conflicts; however, developing, refining, employing, and mastering those technologies are far more complex and serious challenges than just opining on their potential. This paper addresses the appeal of new technology for military applications, but with a healthy dose of technical reality through a Chinese frame that must be acknowledged and considered.

Technical reality matters because the inspiration of emerging technologies can tempt skipping over the challenge and hard work required to transform research from concept to use. As realities of past conflicts with peer adversaries fade from national consciousness, so too has an awareness of the physical and intellectual endeavors and investments that placed the United States in a unique position of wealth and power. We have also forgotten just how closely run those competitions were. Moreover, the intricacies and complexity of modern technologies demand more nuanced technical understanding by senior leaders, policymakers, and operators who will contemplate their use, fully employ their unique capabilities, and fold them into national strategies.

The Chinese frame we adopt matters for two reasons: first, we are competing with China economically, politically, technologically, and militarily; and second, and more pointedly, we believe China's ability to disrupt the world order we favor is enabled by the highly integrated information technology strategy they are doggedly pursuing.

Strategic Context

The United States, once again, faces peer competitors, and the National Security and Defense Strategies of the current administration are explicit in this regard. The bipartisan National Defense Strategy Commission appointed by Congress agreed with that assessment but found the National Defense Strategy short on innovative concepts and analysis. It can be inferred from the strategic documents that Russia and China are both on par as competitors, but the rise of China presents the greatest challenge to the United States and the nature of the global order. China, following the pattern of past rising powers, is in an expansionist stage as it reemerges as a Eurasian land power with the desire, policies, and associated investments to also extend its influence on the oceans of the world. Its strategic approach melds the thinking of the geostrategist Halford Mackinder and the navalist Alfred Thayer Mahan, flavored with the timeless influence of the Chinese military strategist and philosopher Sun Tzu, who opined that "strategy without tactics is the slowest route to victory, tactics without strategy is the noise before defeat."

China's approach encompasses both strategy and tactics. It is at once simple and complex, a blend of geo-economic moves with geopolitical consequences. It is facilitated by a generally benign security environment and norms created and upheld by the United States and its network of alliances. China has benefited from two decades of the United States suppressing terrorism—avoiding expending blood and treasure in that protracted conflict—and has shaped its military to exploit perceived gaps and vulnerabilities in United States and regional allies' capabilities. China thrives in the "gray zone"—the continuum between peace and war where power is asserted and influence is gained or lost without resorting to overt military force. This is a challenge for the United States as our view of conflict is binary: hot or cold. China sees conflict as fluid and hews to Sun Tzu's adage to subdue the enemy without fighting.

Importantly, China's rise has been enabled and accelerated by extraordinary advances in technology that have allowed it to skip fortuitously over generations of dated technologies and models upon which the United States continues to depend. This has facilitated a broad national agenda that recognizes the power of technological primacy, particularly information technology. New information infrastructure and applications, overlaid on its Belt and Road Initiative, put China in a position to extend its influence in telecommunications, information systems, and e-commerce in developing countries and strategically significant locations (including space) on a consequential scale.

A frequent trope is that China's technological advancement is primarily the result of stealing intellectual property. China has benefited greatly from that theft and coercive business practices, and that execrable behavior must be stopped. However, we must accept the reality of China's prowess in technological innovation and, importantly, the application of their legitimate efforts. China's current investments and innovation in artificial intelligence (AI), microprocessors, 5G, quantum science, and space technology are significant, genuine, and strategic and are poised to become preferred solutions for other countries to adopt. Their innovations could end up serving as the infrastructure of the future information society and position China for technological and political advantage should its standards, systems, and policies be adopted widely by others.

The Information Imperative

Our last peer competition, the Cold War with the Soviet Union, turned on nuclear and ideological strategies. Today we compete where the outcome will be dependent upon information—how it is generated, obtained, transported, integrated, and used. While we acknowledge the importance of technical advancements in kinetic weapons, and China's accomplishments in that portfolio are impressive and lethal (e.g., hypersonics, undersea systems, and missile defense), technologies that define the information environment are the coin of the realm, especially in the gray zone. The information technology competition will change the nature of conflict and the definition of winning and will have profound economic, political, and military consequences. If we do not approach information in warfare as an imperative and keep our defense preparations in motion, if there is not a broad appreciation of what those preparations demand, the future way of war will be a shock to the American people.

Fueling the Strategic-Technical Competition

The Cold War challenged the United States, but strategic consensus, coherent policy, pragmatic investment, and scientific and technical leadership prevailed. Competition with the Soviet Union inspired, indeed required, military and nonmilitary technical innovation. It stimulated agreeable and productive cooperation among government, academia, and industry. Unfortunately, these premises no longer hold true.[1]

More so than in the past, U.S. private research and development organizations are leading technology development, and there is an expectation, perhaps more a hope, that the U.S.-born technology giants will contribute to our nation's military edge. The investments and productivity of the research arms of Google, Amazon, Apple, Facebook, IBM, and others are indeed impressive but so too are the investments of Baidu, Tencent, Alibaba, and Huawei, among others. Moreover, the world-class talent that drives discoveries and developments globally has demonstrated a willingness to join the company with the most exciting research, regardless of national affiliation.[2]

Although Chinese and U.S. companies are both making considerable investments in R&D, the application of that R&D for national security differs in important ways. China is overt in its approach of state-directed military–civilian cooperation. President Xi Jinping has bluntly stated, "implementing the strategy of military–civilian integration is a prerequisite for building integrated national strategies and strategic capabilities and for realizing the Party's goal of building a strong military in a new era."[3] While China is forcing shared technology, our alternative of cooperation of the willing in combining commercial and military technology, as was done in the years after World War II and the Cold War, seems outdated. American companies are, at times, unwilling to even entertain contracting with the Department of Defense or share new technical capabilities or information. The impediments of an onerous military procurement model certainly contribute to this predicament. Incentives for U.S. corporations to reach global markets also drive them to different decisions than their Chinese counterparts, who are given more compelling national incentives.

Intellectual Capital

The United States benefited from significant investments in higher-level and technical vocational education after WWII. That boost, fueled by a generous GI Bill, accelerated innovation and the capacity and competence to lead globally in highly technical areas. China is emphasizing and spending heavily on education today and has turned to Western universities for much of that intellectual stimulus. In the United States from academic year 2007–2008 to 2017–2018, the number of Chinese students in the United States rose from 81,127 to 363,341.[4] Beyond numbers, it matters what is being studied. China surpassed the United States in natural sciences and engineering doctoral degrees attained in 2007 and remains ahead today.[5] More worrisome is the decline in the number of U.S. citizens majoring in academic disciplines that underpin information technology. In 2017, U.S. graduates in computer science and electrical engineering comprised 21% and 19% of graduating students, respectively; all other students were foreign.[6] How China and the United States build intellectual capital will drive innovation. An indication of that drive can be seen with the 1.34 million patent applications in China in 2017, compared to 605,000 in the United States.[7] Beyond patents, a more technically literate public will be more comfortable, productive, and cyber-secure in the "internet of things" environment, where information will be more central to the new way of life and of war.

Taiwan—20XX. What if?

The allure of the promise of new technology in war often results in speculation regarding how a particular technology could be used offensively or defensively. In turn, that enables advocates to give their favored technology the aura of a "silver bullet." It is easy to give cyber, autonomy, or AI an outsized role. The future way of war will be complex and must be envisioned or imagined through a new lens that combines multiple information technologies with kinetic weapons in new ways.

In a conflict with China, no scenario is more stressing or will be harder fought than that of the forcible reunification of Taiwan with mainland China. A glimpse of the old version of such a move previewed in 1996 when the People's Republic of China (PRC) displayed its displeasure over Taiwan's drift from the One-China policy and fired missiles into areas near Taiwan. The United States responded easily and confidently by positioning naval forces near the island, giving PRC leadership pause.

That was two decades ago. What if, within two decades from now…

- President Xi chose to realize the long-held belief that Taiwan be reunited with the mainland?
- Social media, e-commerce sites, and the social credit score system have been used to sharpen Chinese public opinion regarding the imperative to reunify Taiwan, to develop unwavering belief in the efficacy of the People's Liberation Army (PLA) to be able to do so, and to emphasize that the time is now to use civil–military information capabilities and protracted investments in PLA kinetic and non-kinetic capabilities to finally bring Taiwan into the PRC?
- Internet and social media policies and practices prevent and stifle views counter to forced reunification?

What if, in the decision to retake Taiwan, China…

- Hosted an open demonstration of a coordinated hypersonic missile/DF-21 strike on a distant at-sea target?
- Deployed double the normal number of PLA Navy submarines in the area while simultaneously increasing patrols in the vicinity of Guam?
- Activated a fixed and mobile undersea sensor wall that would track the movement of U.S. naval forces into the area?
- Targeted the families of U.S. sailors at sea in the region in ways that caused bank, credit union, and credit card accounts to be frozen?
- Used targeted social media posts with harmful content that eroded U.S. and allied confidence in deployed military capability?
- Promulgated precisely targeted adverse information across multiple platforms about U.S. leaders in the midst of a contentious election?
- Interrupted electrical power on Taiwan, Guam, Hawaii, and the U.S. West Coast—affecting important naval and air bases and corporate headquarters?
- Caused a flash crash of the S&P 500?
- Disrupted U.S. GPS (but not the BeiDou system) by inserting inaccuracies that disrupt U.S. and allied military forces, commercial aviation and shipping, and regional military and commercial autonomous vehicles?
- Caused loss of control and un-commanded shutdowns of U.S. unmanned systems resulting in crashes of numerous vehicles, some in populated areas?
- Slowed or redirected specific containers in the ports China operated, disrupting U.S. military logistics and U.S. and other manufacturing supply chains?
- Flooded the area around Taiwan, the East China Sea, and the South China Sea with PRC Coast Guard and Maritime Militia ships in coordination with People's Liberation Army Navy ships?
- Genetically altered the algae bloom in the East China Sea to change colors to indicate when a non-Chinese warship is passing?

- Deployed autonomous swarms of unmanned aerial vehicles in the Strait of Taiwan and the Strait of Malacca?
- Employed soldiers genetically altered to be more resilient to normal battlefield conditions?
- Repositioned space assets in the western Pacific and western approaches to the Strait of Malacca, some extremely close to critical U.S. space sensors?
- Conducted coordinated cyber and electronic warfare jamming of U.S. sensors and networks supporting operations in the western Pacific?
- Disabled and destroyed key components in machinery control systems of U.S. ships operating near Chinese Maritime Militia units?

Hypothetical, yes; feasible in the 20XX timeframe, yes. Each move is at least provocative, and collectively they are daunting and require a broad national strategy that transcends purely military considerations.

Strategy and Technology

> *The [Chinese] Strategic Support Force consists of space, counter-space, cyber, offensive cyber, intelligence, surveillance and reconnaissance, all in a single command. Why did they do that? Because they understand the need to integrate information.*
>
> — General John Hyten, United States Air Force[8]

So, what is the technology strategy needed to engage in a competition, likely a gray-zone competition, with a near-peer focused on "information power"? The preferred outcome, especially should the United States be forced into a kinetic engagement, would be a quick, decisive, and public rebuke of Chinese military capability and leadership. While we do not presume to offer the strategy needed for this outcome, we do seek to inform a conversation that must happen among strategists, operators, and technologists regarding the role of information.

The technologies we examine play across the life cycle of information: how we collect it, secure it, manipulate it, defend it, share it, process it, integrate it, and act with it. The technologies generally fall into three categories: technologies for kinetic use in the theater of military operations, technologies relevant to homeland protection, and technologies relevant to a global influence campaign. Furthermore, in a conflict with China we assume that engagements or encounters will lack boundaries—geographic, military or civilian, diplomatic, economic, or demographic.

Complicating the situation, the competition to dominate in emerging technologies has a feature specific to our time: speed. The pace is driven in part by worldwide commercial investments and the intersection of changes in disparate fields through the global exchange of research. These investments are mentioned throughout because they are important to understanding the resources that might lead to breakthroughs. However, we should keep in mind that while U.S.-based companies are incentivized to pursue global markets, Chinese companies are incentivized to ensure China's national interests are met.

AI and Autonomous Systems

Why These Technology Developments Matter

AI and autonomous systems could be the differentiating factor in a conflict. They could affect the entirety of the information life cycle—how we collect it, secure it, manipulate it, defend it, share it, process it, integrate it, and act with it.

Expanding and collapsing the decision space. AI can speed up everything from jamming modalities, to mine identification and defeat, to intelligence analysis, or, more broadly, to financial transactions. In a kinetic engagement, the ability to act within our adversary's timeline (referred to as the OODA [observe–orient–decide–act] loop) confers great advantage. Conversely, AI and autonomy could help exploit short timelines by rapidly synthesizing information to predict next moves. For example, recent work has focused on machine learning (a subset of AI) for real-world event prediction. Bringing together data from local news, social media, press releases, and sensors could help intelligence officers anticipate gray-zone operations or combat preparations, just as they have been used to predict civil unrest.[9] Early analysis suggests that new elements of the Chinese Belt and Road Initiative can be understood and predicted using specialized algorithms on large datasets.

Raids. Large-scale, rapid-fire command and control for multi-domain systems over multiple fronts is hard to achieve, but would be incredibly useful in overwhelming an opponent. The size of the Chinese arsenal in theater makes raids an appealing tactic for China—one that can be made more lethal by autonomy. Autonomy is also key to future missile defense capabilities that must coordinate a rapid reaction by sensors, weapons, and platforms. These sorts of capabilities are being worked in laboratories and in test exercises today.[10]

It is also interesting to consider how AI-enabled influence operations could combine AI's advantage in speed and widespread coordination. AI and machine learning are demonstrating significant potential in scaling or defending against influence campaigns. Marketing and political campaigns have already demonstrated uses of AI in shaping public opinions in real time and with bespoke content. More than that, deep fakes—videos that leverage AI to create believable but fictional videos, for example, about the president—could become a powerful weapon in an information campaign.[11] Similarly, just as AI can help to exploit information, it can also be used to exploit weaknesses in other AI systems. This is a newer area of research but one holding great promise.[12]

Looking farther ahead, there is the potential for merging AI breakthroughs with breakthroughs in bioengineering, such as CRISPR-Cas9 genome editing. While this may seem futuristic, given the tools being developed today, it may not be too distant a step. For example, instead of relying on generating wet lab mutations to create new biological capabilities (e.g., bioengineered sensors to detect ship movements), we might instead capture physical space biological details in the information space. Then, with an assist from AI, the information space representations could be deeply modeled, manipulated, and explored. When a satisfactory result was achieved, we could then transition back from the information space to the physical space, with an assist from CRISPR-Cas9, to create the desired biological capability. In fact, the potential to rapidly create a variety of new biological capabilities would be immense.

Together, these and other uses of AI in a kinetic fight, in defending the homeland, or in global influence operations would help to satisfy a political precondition of a fight for either side: that it be quick, decisive, and ultimately deflating to the adversary.

The Technical Race

The United States once had a clear and growing advantage in the realm of AI, but that advantage has been whittled away. There is still good reason to believe that the United States could maintain an edge, although it would be admittedly small. It is now important to consider the repercussions of China attaining its stated goal to lead the world in AI by 2030.

The intellectual capital of the United States, one of our core strengths as a nation, may be the greatest reason for hope. Our academic papers are still the most respected, and our universities are still leaders in the field. While we should be justifiably worried about the state of higher education for achieving an AI-enabled and highly autonomous future, we still operate from a position of strength, and we can maintain an edge if we put forth the effort.

Other strengths that should not be overlooked are our alliances and the intellectual capital of our allies. Europe is the largest publisher of AI papers, and 12 of the top 20 companies filing AI-related patents are based in Japan (three are from the United States, and two are from China). Lest we get too comfortable, however, Chinese universities make up 17 of the top 20 academic institutions filing for AI-related patents.[13]

Finally, that China has more access to data to train their AI algorithms is not a reason to believe that the United States will lose this race. There are ways to develop this technology without sacrificing our nation's foundational principles.[14] In particular, transfer learning techniques (transferring machine-learning algorithms from one application to another) and techniques to create synthetic and proxy data are demonstrating that large quantities of data is not the resource it was once feared to be. Some of the most exciting work in machine learning today—and the most applicable to military needs—is being done with what has been referred to as "enormously small data."

Questions to Ask

AI advances are tangible, but there is still a gulf separating the research and development of AI from military operations. While it is good sport to blame the U.S. defense acquisition process for this gap, there are practical, technical, and ethical factors that must also be considered.

How will AI integrate into the systems we have? And when should new AI systems replace legacy systems? Billions of dollars have been invested by American taxpayers to create current capabilities and platforms. Those platforms are complex, and dropping in the newest piece of code or hardware is no simple task. It can generate a cascade of system changes and time-consuming validation tests. There is, however, promise in the example of past designs for modularity and upgrades, such as the Submarine Acoustic Rapid Commercial Off The Shelf (COTS) Insertion program, but the applications are few.

How will our operators use it? Will our commanders trust it? Research on the challenges of human–machine interactions and human–machine integration is progressing, but leadership must carefully consider how operational commanders will or should delegate decision-making to an autonomous system. Current policies regarding control of lethal force and the military's culture of accountability and responsibility make trusting an autonomous system to make life-or-death decisions difficult.

How do we know it will work as intended? How should it be verified and validated for use? Despite progress in laboratories, real-world applications continue to demonstrate the fragility of current autonomy. We are still at a point where autonomous systems fail to perform as expected under novel conditions, and it is hard to predict when a situation will become novel to an autonomous system. This may be acceptable for a robotic vacuum cleaner, but it is not for an advanced unmanned fighter. While technologists are working to overcome these challenges, they still remain. In addition, current test and evaluation methodologies must be updated because current approaches may no longer be effective.

What does it mean to have "meaningful control" over an autonomous system? No technology should be fully developed or deployed without due consideration for how it might be used or misused. Ethical, legal, and policy guidance for "meaningful human control" of U.S. autonomous systems is nascent. That guidance can and should influence technological developments. However, we must be aware of the artificial asymmetry that might be introduced if we overly constrain our use of autonomy and China does not. This is an area where policymakers and technologists, together, must rigorously examine assumptions and likely consequences.

Space Technologies

Why the Technology Matters

Space-based assets underpin much information power by providing infrastructure for transferring information and the essential positioning, navigation, and timing information needed for U.S. and Chinese forces to operate effectively and employ precision weapons. As the commander of the U.S. Strategic Command, General John Hyten, put it, "access to space underpins our ability to project power globally, strike targets precisely, and discern and respond to threats before they endanger the homeland or U.S. global interests."[15] Beyond military applications, American reliance on space assets has been compared to our reliance on electricity: relevant to so many aspects of life—financial networks, weather monitoring, navigation, and more—but only noticed when it is absent.[16]

Despite the importance of our space assets, Hyten will admit: "we didn't build our systems for a contested environment."[17] And in a conflict with China, where our forces will operate far from the homeland and be especially reliant on satellites to fight effectively, space could be a highly contested domain.

The Technical Race

While the United States remains dominant in space, there are many examples of a vigorous challenge to that dominance. According to a May 2018 report of the Xinhua News Agency, more than 60 Chinese commercial space companies have entered the market in the past three years.[18] China launched 35 rockets into Earth orbit last year—more than any other nation.[19] In early 2019, China completed the first-ever landing of a lander-rover on the far side of the moon, a source of great national pride and international prestige. The Chinese space agency is now preparing for the launch of the first module of the Chinese Space Station as well as the first independent Chinese mission to Mars.

Approximately half of the satellites recently launched are part of the Chinese-developed BeiDou positioning system. An independent global positioning and navigation system has obvious security advantages for China and grants it independence from the U.S. GPS. BeiDou also has considerable economic implications as a piece of China's Belt and Road Initiative. Closer to home, BeiDou is useful for Chinese internal stability and surveillance efforts. With these advantages, however, come vulnerabilities to China's space-based assets.[20]

Chinese investments go ominously beyond satellite development. Chinese anti-satellite (ASAT) development is a known and growing challenge to U.S. reliance on space-based assets. Some of the details about their development have not been kept a secret, as the 2007 Chinese satellite intercept and 2014 ASAT test visibly demonstrated.[21]

Regardless of the U.S.–China dynamic, space technologies and investments worldwide are moving quickly. The number of satellites in space increased 50% over the five-year period from 2013 to 2017.[22] This complicates situational awareness and freedom of action in space.

Questions to Ask

Is a new system or architecture defensible and resilient? The U.S. reliance on space is a known strength and vulnerability. Debates and analyses have been focused on evaluating the relative merits of varying degrees of resilience and defense options for space-based assets. Before deploying space-based information assets, we must question to what degree they must be defended. We must also declassify and more broadly share information regarding the space-based capabilities of others, so the American public can appreciate how contested space has become and what we must do to win in that vital domain.

Cyber Offense/Defense

Why It Matters

While autonomy and AI may be viewed as the ability to process and act upon data, cyber can be viewed as the network that contains and enables the sharing of data. As such, it is vital to the information lifecycle. Competition in the cyber domain is not new, but the technology continues to evolve in important ways. Those developments have significant implications in potential kinetic engagements and broad-reaching consequences for homeland defense and influence operations.

As a recent Defense Science Board study succinctly put it, "defense is a necessary foundation for offense."[23] The need for good cyber defense applies far beyond military platforms, classified networks, supply chains, intellectual property, and the personal information of government personnel. Good cyber defense enables every military purchase and operation.

Cyber operations are not limited by traditional notions of the battlefield, or by military and civilian combatants. If China wished to create a domestic distraction immediately prior to an operation in the Pacific theater, a cyber operation that was not attributable to a government entity would be a good way to do it. Moreover, as the connection between bio and information grows stronger, the mass of genetic and healthcare data could be an enticing target that could be disclosed or manipulated to create targeted or widespread harm.

Cyberattacks could also change in important ways with the advent of 5G networks, which China is focusing on as a key technology. These networks are far more than 4G. The speed 5G enables positions it as the critical infrastructure for the internet of things and for civilian and military uses. As a core element of the future autonomous world, 5G networks are an especially attractive target for the collection, manipulation, and sharing of data.

The Technology Race

Both China and the United States are pursuing offensive and defensive cyber capabilities for military applications, and it is apparent both countries are competent and continually developing new capabilities. While directly comparing advances being made in the offensive area is difficult, cyber defense can be more readily assessed.

Advances in autonomy for cyber defense offer hope of improving system defenses. Efforts to automatically discover and share vulnerability information across the private sector and with government are helping to alleviate more mundane and nuisance issues in industry, which faces a morass of security software offerings that require complicated integration to work effectively.[24]

Research is also emerging that suggests that monolithic software systems—dangerous because one attack vector can affect or access so much—might also be reasonably diversified to confound far-reaching attacks. Many attacks can be mitigated by diverse code generation techniques or by using different hardware and software offerings to achieve the same functionality, which introduces a higher degree of resilience but is often hard to achieve at a reasonable cost (both in creating and maintaining the diverse systems).

In comparing the technology race for cyber in the United States and China, we must also consider education in cyber-related fields. For example, a 5G environment demands more than just basic computer literacy to maximize the use of that technology, improve self-defense, and create a more cyber-competent military force. We must be mindful that while U.S. universities still dominate international rankings boards for computer science, there has been incredible progress by top Chinese universities.[25]

Questions to Ask

When cyber offense and defense are in a zero-sum game, what is the right balance between them? While improving cyber defense is a strategic issue on the battlefield and at home, cyber has an inherent challenge regarding "equities." In certain instances, disclosing a vulnerability in a commercial system can strengthen security at home but disadvantage offensive cyber operations against an adversary. This is an important challenge and one for which various processes have been developed.[26] Beyond individual cases, however, how should we balance system-wide resilience and military options in conflict?

Who has the authority to decide? Who, or what entity, has the authority to coordinate a whole-of-government response? Authorization and organization for a national cyber response are unclear. The speed of action and reaction require preplanned and carefully assessed actions. Such plans transcend any one department or agency and must be developed with urgency. Similarly, at operational and tactical levels, clearly designating who has the authority to act and be accountable is a challenge. Moreover, creating seamless and coherent integrated cyber and kinetic response schemes and protocols remains an important issue.

How much defense is enough? The challenges of cybersecurity are so pervasive that the idea of returning to the old world of paper, pen, and in-person meetings is sometimes tempting. But short of that extreme, it is difficult to know how much defense is enough. One point for leaders to consider is not how much but rather where should we invest in defense. As the Office of Personnel Management hack demonstrated, the need for defense goes beyond Department of Defense systems. And as the Sony Pictures hack and subsequent threats demonstrated, the national security need goes beyond the government.

Another question in cyber relates to our discussion of autonomy: what qualifies as "meaningful human control" of an autonomous cyber defense system? Autonomy will be necessary to identify threats and respond at computer speeds to counter attacks and protect data. In the instance of a flash crash, a system reset may be acceptable, but it is unlikely that many situations will be so straightforward. Moreover, even when a system reset is possible, the large amount of time often required for resets in legacy systems may cause planned responses to be overcome by events.

Quantum Technologies

Why the Technology Matters

If autonomous systems and AI are atop the list of consequential technologies today, quantum computing is often cited as the next big thing, and perennially has been 20 years away (although not all are so pessimistic). That quantum technology often tops technology wish lists, despite the challenges and uncertain timing, is an indication of its revolutionary potential for information power in terms of capacity, sensitivity, and speed.[27] In addition to quantum computing, there are other quantum technologies, such as quantum key distribution for quantum encryption and quantum sensing, that have been developed and have the potential to impact operations in the nearer term.

Quantum computing could revolutionize our ability to process data for different types of modeling, simulations, and optimization. This would have a considerable effect for research and development on everything from pharmaceuticals to materials to weapons systems. The applications would also stretch to the equally important issue of optimizing supply chains, something that could enable resilient, disaggregated logistics, which would be especially useful for long logistics lines in the Pacific.[28]

Quantum computing, when it comes to fruition, will undermine modern public-key encryption systems. With this, there could be a significant first-mover advantage: whoever gets this technology first will have access to public-key encrypted information around the world, unless a "post-quantum" infrastructure is put in place beforehand.

Conversely, quantum encryption could enable secure communications. China has made progress on this, having demonstrated intercontinental quantum-enabled communication in early 2018.[29] Recent research suggests, however, that there may be vulnerabilities in many quantum cryptography systems that could diminish their advantage over more traditional, mathematical cryptography approaches.[30]

The quantum capability most likely to be realized in the near term is quantum sensing. This is of significant interest because of the centrality of sensors to the Chinese anti-access/area-denial strategy. These sensors have already proven themselves by enabling exquisitely accurate atomic clocks. Forecasts suggest that accuracy limits have not been reached, and one laboratory has demonstrated an atomic clock with a timing error of less than one second in five billion years.[31] With these clocks and new quantum sensors sensitive enough, for example, to detect the Earth's magnetic field at a given point, researchers are imagining replacements to vulnerable space-based GPS assets.[32] Moreover, quantum sensors could enable sensitivity and resolution that could detect underground tunnels and bunkers, as well as enable commercial uses for mineral deposits or health diagnostics.[33]

The Technical Race

There are significant interlocking technical advances that must be made to realize the full potential of quantum computing, which makes it difficult to predict when future quantum capabilities will be realized. However, the literature on quantum information sciences (QIS), global investments, and public pronouncements indicate increasing momentum.[34]

China and the United States have committed publicly to quantum research and are investing significantly in it.[35] The United States recently passed the National Quantum Initiative Act, and China recently opened a $10 billion quantum research supercenter. Similarly, the European Union has its own "Quantum Manifesto" and is making considerable investments.[36] Commercial activity also indicates a growing market for quantum technologies, and Alibaba, one of China's largest companies, has invested significantly in the technology.

Questions to Ask

How should we prepare for a post-quantum world? It would be wise to begin preparing encrypted systems for a post-quantum world. The "should" in the question, however, speaks to the timeline issue associated with quantum technologies. As Jim Clarke, the director of quantum hardware at Intel Labs, put it:

> *The first transistor was introduced in 1947. The first integrated circuit followed in 1958. Intel's first microprocessor—which had only about 2,500 transistors—didn't arrive until 1971. Each of those milestones was more than a decade apart. People think quantum computers are just around the corner, but history shows these advances take time.*[37]

Other Technologies Relevant to the Information Competition

Electronic Warfare and Directed Energy

While the technologies we have discussed are important to an information competition with China, our list is by no means exhaustive. There are many other information-relevant technologies that also have merit. For instance, it would be nearly impossible to move, communicate, coordinate, or strike against a capable adversary without assured access to reliable electromagnetic capabilities. As an example, the electronic warfare (EW) capabilities developed by China are a formidable obstacle that could significantly degrade the U.S. military's ability to respond to Chinese offensive operations.

Conversely, EW that is aggressively developed and employed strategically by the United States could enable dominance by disrupting Chinese sensor and weapon networks and degrading the PLA's ability to conduct precision operations and strikes. If subject to jamming, deception, and other EW attacks, the PLA would be forced to use more forces and expend more munitions in an effort to achieve the same military result.

On a related note, directed energy (DE) must also be considered for its potential to disrupt information. The research, development, test, and evaluation funding for DE weapons in the United States in 2018 "increased 23 percent relative to 2017." China's investments have also had observable effects.[38] The potential of the technology is currently limited by its inability to maintain beam intensity beyond relatively short ranges and its restriction to line-of-sight targets.

Weapon/Domain-Specific Technologies and Information

Any conversation about competition with near-peer adversaries today is incomplete without mentioning hypersonic weapons and undersea warfare. In both, the acquisition, processing, and communication of information is essential to success. Defense against hypersonic weapons requires information capabilities that can predict, acquire, target, and enable an engagement decision at speeds that challenge our current capabilities.

Maintaining the edge undersea will also require the development and deployment of technologies needed for information dominance—AI and autonomy, space, cyber, quantum, and EW—to protect our assets and detect and track our adversaries. While not explicitly called out in the top-10 list of technology and research priorities of the Under Secretary of Defense for Research and Engineering, undersea requires focused attention. While the United States clearly maintains a significant lead undersea, China recognizes this and is working aggressively to shrink and neutralize our lead. If we do not continue pursuing disruptive development in all facets of undersea operations, we will give up significant strategic, operational, and tactical advantages.

What Lies Between Good Ideas and Good Outcomes

This paper has highlighted the increasing centrality of information in modern warfare and how innovation in that area will change the nature of conflict, taking the contest beyond the boundaries and norms of the past. As a nation with global interests, obligations, and responsibilities, we will confront different challenges and threats in the Pacific and beyond, singly and in concert with others. While the technologies we bring to bear in each circumstance will vary, information will be more central to both offense and defense than ever before.

Our hypothetical scenario implies a new kind of conflict, one that is global in nature with greater non-kinetic means to influence and compel on a global scale in multiple domains. The technologies we discussed are equally pressing and global. Yet, sadly, our scenario and the technology needs are additive to the protracted conflict in the Middle East and security challenges sure to arise elsewhere. In parallel, leaders must understand the complexities of global strategies and global technologies and how they interplay.

National security leaders will face louder calls to think anew and cast off legacy systems, to be revolutionary rather than evolutionary, and to bet on the promise of new technology and, by doing so, greatly reduce the cost of defense. But warfare has never been purely revolutionary. Regardless of how information will change the nature of conflict, the military capability we and our adversaries have today will not all be jettisoned and replaced en masse with the technologies we described. The key will be how quickly we evolve and how prepared national security leaders and operators are—intellectually and culturally—to effectively employ innovation for information dominance. Our challenge is to be proactive in capitalizing on technology trends and not simply reactive to adversary developments, and to focus as much, if not more, on rapid adoption and integration as we do on the breakthrough technology itself. We must alter incentives so that speed in discovery and its transition to application are valued above adherence to a highly refined but risk-averse acquisition process.

The changed pattern of technical innovation with significant developments originating in the nondefense sector must be acknowledged and leveraged more effectively. The period of civil—military cooperation that produced noteworthy breakthroughs and that is accelerating the application of defense technology in China must become a priority of our government and the U.S. private sector.

Academia must examine its responsibility and obligation to national security, including how it develops relevant intellectual capital in future generations in technical and policy areas, how it inspires and prepares U.S. students to pursue technically rigorous courses of study, how it supports research and policy in areas vital to national defense, and how it deals with students and financial support from potential adversary nations. The current absence of academia in the national security equation is filled by think tanks, which are not well-equipped to cultivate the number of future practitioners needed to ensure our interests in the years ahead. At a time when we are being economically, politically, technically, and militarily challenged in ways not seen for decades, we need stronger voices in university leadership who explicitly call for keeping defense preparations in motion.

The imperative of allied and coalition interoperability and research collaboration will be more important in future information environments and networked operations. Our policy and processes do not adequately incent collaboration among relevant Pacific allies. Speed of cooperation, ease of disclosure, and fewer restrictions on the originators' intellectual property must be at the top of the policy list. This will not be easy, but without realizing full and seamless interoperability in the information domain, attempts at combined operations in the future may diminish effectiveness.

Finally, strategy and technology wear dollar signs for friend and foe alike. Our all-volunteer force wears one much greater than the competitors and adversaries we face in multiple regions. We will not find it easy nor in our national interest to be away from key regions, despite the expense. Allied capability and capacity in regions of import are helpful but do not appreciably change the military balance nor are they robust enough to swing to other regions especially if competitors cooperate. Streamlined procurement and infrastructure will relieve some pressure on our national security budget but will not be a panacea. In time, if we are efficient and more collaborative at a national level in accelerating the technologies we discussed, we can evolve the design and nature of our force, but we must also recognize that the new battlespace will require investments to be made in military and nonmilitary information infrastructure and human capital. This brings us back to where we began: this is indeed a national challenge that requires a national strategy that is the collective responsibility of our society.

[1] Richard Danzig, John Allen, Phil DePoy, Lisa Disbrow, James Gosler, Avril Haines, Samuel Locklear III, James Miller, James Stavridis, Paul Stockton, and Robert Work, *A Preface to Strategy: The Foundations of American National Security* (Laurel, MD: Johns Hopkins Applied Physics Laboratory, December 2018), https://www.jhuapl.edu/Content/documents/PrefaceToStrategy.pdf.

[2] Josh Horwitz, "Baidu's Artificial-Intelligence Wizard, Andrew Ng, Has Resigned from China's Search Giant," Quartz, March 22, 2017, https://qz.com/939025/baidus-artificial-intelligence-wizard-andrew-ng-has-resigned-from-the-company/.

[3] 13th National People's Congress, March 12, 2018.

[4] U.S. Department of State Bureau of Educational and Cultural Affairs and Institute of International Education, "2018 Fact Sheet: China," https://www.iie.org/Research-and-Insights/Open-Doors/Fact-Sheets-and-Infographics/Leading-Places-of-Origin-Fact-Sheets.

[5] National Science Board, *Science and Engineering Indicators 2018*, NSB-2018-1 (Alexandria, VA: National Science Foundation, 2018), https://www.nsf.gov/statistics/indicators/.

[6] *H-1B Visas by the Numbers: 2017-18* (Arlington, VA: National Foundation for American Policy, April 2018), https://nfap.com/wp-content/uploads/2018/04/H-1B-Visas-By-The-Number-FY-2017.NFAP-Policy-Brief.April-2018.pdf.

[7] *World Intellectual Property Indicators 2017* (Geneva: World Intellectual Property Organization, 2017), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2017-chapter2.pdf.

[8] John Hyten, "U.S.STRATCOM at DoDIIS Worldwide Conference," U.S. Strategic Command, August 13, 2018, http://www.stratcom.mil/Media/Speeches/Article/1607422/usstratcom-at-dodiis-worldwide-conference/.

[9] See, for example, IARPA's Geopolitical Forecasting Challenge, https://www.iarpa.gov/challenges/gfchallenge.html.

[10] "Department of Defense Announces Successful Micro-Drone Demonstration," U.S. Department of Defense, January 9, 2017, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/.

[11] Robert Chesney and Danielle K. Citron, "Disinformation on Steroids," Council on Foreign Relations, October 16, 2018, https://www.cfr.org/report/deep-fake-disinformation-steroids.

[12] Wojciech Czaja, Neil Fendley, Michael Pekala, Christopher Ratto, and I-Jeng Wang, *Adversarial Examples in Remote Sensing*, May 29, 2018, arXiv preprint arXiv:1805.10997, https://arxiv.org/pdf/1805.10997.pdf.

[13] Yoav Shoham Raymond Perrault, Erik Brynjolfsson, Jack Clark, James Manyika, Juan Carlos Niebles, Terah Lyons, John Etchemendy, Barbara Grosz, and Zoe Bauer, *The AI Index 2018 Annual Report* (Stanford, CA: AI Index Steering Committee, Human-Centered AI Initiative, Stanford University, December 2018); *Technology Trends 2019: Artificial Intelligence* (Geneva: World Intellectual Property Organization, 2019), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf.

[14] Danzig et al., A Preface to Strategy.

[15] *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Washington, DC: United States Institute of Peace), https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf.

[16] H.A.S.C. No. 115-28; Serial No. 115-12: Threats to Space Assets and Implications for Homeland Security, Joint Hearing Before the Subcommittee on Strategic Forces of the Committee on Armed Services Meeting Jointly with Subcommittee on Emergency Preparedness, Response, and Communications of the Committee on Homeland Security, House of Representatives, 115th Cong., First Session, Hearing Held March 29, 2017, https://www.hsdl.org/?abstract&did=806644; The White House, National Security Strategy of the United States of America, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[17] Sandra Erwin, "Q&A: Air Force Gen. John Hyten Says U.S. Space Strategy, Budget Moving 'Down the Right Path'," *SpaceNews*, April 3, 2018, https://spacenews.com/qa-air-force-gen-john-hyten-says-u-s-space-strategy-budget-moving-down-the-right-path/.

[18] Bruce Einhorn and Dong Lyu, "Space: China's Final Frontier," *Bloomberg Businessweek*, no. 4589, October 22, 2018, 14–15, http://search.ebscohost.com.proxy1.library.jhu.edu/login.aspx?direct=true&db=bsu&AN=132474262&site=ehost-live&scope=site.

[19] Joan Johnson-Freese, "China Launched More Rockets into Orbit in 2018 Than Any Other Country," *MIT Technology Review*, December 19, 2018, https://www.technologyreview.com/s/612595/china-launched-more-rockets-into-orbit-in-2018-than-any-other-country/.

[20] Eric Hagt, "China's Beidou: Implications for the Individual and the State," *SAIS Review of International Affairs* 34, no. 1 (2014): 129–140, https://muse.jhu.edu/article/547669/pdf; Pratik Jakhar, "How China's GPS 'Rival' Beidou Is Plotting to Go Global," *BBC News*, September 20, 2018, https://www.bbc.com/news/technology-45471959.

[21] Ryan Browne and Barbara Starr, "U.S. General: Russia and China Building Space Weapons to Target U.S. Satellites," *CNN*, December 2, 2017, https://www.cnn.com/2017/12/02/politics/russia-china-space-weapons/index.html; John Hyten, "U.S. Strategic Command Space and Missile Defense Symposium Remarks," U.S. Strategic Command, August 7, 2018, http://www.stratcom.mil/Media/Speeches/Article/1600894/us-strategic-command-space-and-missile-defense-symposium-remarks/; Colin Clark, "Chinese ASAT Test Was 'Successful:' Lt. Gen. Raymond," *Breaking Defense*, April 14, 2015, https://breakingdefense.com/2015/04/chinese-asat-test-was-successful-lt-gen-raymond/.

[22] Einhorn and Lyu, "Space: China's Final Frontier."

[23] Department of Defense, Defense Science Board, *DSB Task Force on Cyber as a Strategic Capability* (Washington, DC: Office of the Under Secretary of Defense for Research and Engineering, June 2018), https://www.acq.osd.mil/dsb/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf.

[24] "Overview of Integrated Adaptive Cyber Defense," Integrated Adaptive Cyber Defense, accessed February 11, 2019, https://www.iacdautomate.org/learn.

[25] Elizabeth Redden, "Foreign Students and Graduate STEM Enrollment," Inside Higher Ed, October 11, 2017, https://www.insidehighered.com/quicktakes/2017/10/11/foreign-students-and-graduate-stem-enrollment; Over eight years, Tsinghua University has risen from world ranking 58 to number 22. Source: "World University Rankings," Times Higher Education, https://www.timeshighereducation.com/world-university-rankings/tsinghua-university.

[26] "Vulnerabilities Equities Policy and Process for the United States Government," https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[27] European Union, *Quantum Manifesto: A New Era of Technology*, May 2016, https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf.

[28] Scott Crowder, "American Leadership in Quantum Technology," Testimony before the House Committee on Science, Space, and Technology, Subcommittee on Research and Technology and Subcommittee on Energy, Washington, DC, October 24, 2017, https://science.house.gov/sites/democrats.science.house.gov/files/documents/Crowder%20Testimony%20FINAL.PDF.

[29] "Chinese Satellite Uses Quantum Cryptography for Secure Videoconference between Continents," *MIT Technology Review*, January 30, 2018, https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/.

[30] Linköping University, "Some Quantum Cryptography Systems Vulnerable to Hacking, Study Shows," Phys.org, December 18, 2015, https://phys.org/news/2015-12-quantum-cryptography-vulnerable-hacking.html.

[31] Joseph Stromberg, "World's Newest Atomic Clock Loses 1 Second Every 50 Billion Years," *Smithsonian Magazine*, May 30, 2013, https://www.smithsonianmag.com/science-nature/worlds-newest-atomic-clock-loses-1-second-every-50-billion-years-85759022/.

[32] Sofia Chen, "Quantum Physicists Found a New, Safer Way to Navigate," *Wired*, November 1, 2018, https://www.wired.com/story/quantum-physicists-found-a-new-safer-way-to-navigate/; Jim Gimlett, "Quantum-Assisted Sensing and Readout (QuASAR)," Defense Advanced Research Projects Agency, accessed February 11, 2019, https://www.darpa.mil/program/quantum-assisted-sensing-and-readout.

[33] Subcommittee on Quantum Information Science, *National Strategic Overview for Quantum Information Science* (Washington, DC: National Science and Technology Council, September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf.

[34] J. Stephen Binkley, "American Leadership in Quantum Technology," Testimony before the House Committee on Science, Space, and Technology, Subcommittee on Research and Technology and Subcommittee on Energy, Washington, DC, October 24, 2017, https://science.house.gov/sites/democrats.science.house.gov/files/documents/Binkley%20Testimony.pdf.

[35] Jeffrey Lin and P. W. Singer, "China Is Opening a New Quantum Research Supercenter," *Popular Science*, October 10, 2017, https://www.popsci.com/chinas-launches-new-quantum-research-supercenter; "Technology Quarterly: Here, There and Everywhere. Quantum Technology Is Beginning to Come into Its Own," *The Economist*, n.d., https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own.

[36] Adrian Cho, "After Years of Avoidance, Department of Energy Joins Quest to Develop Quantum Computers," *Science*, January 10, 2018, http://www.sciencemag.org/news/2018/01/after-years-avoidance-department-energy-joins-quest-develop-quantum-computers; Paulina Glass, "Congress's Quantum Science Bill May Not Keep the U.S. Military Ahead of China," *Defense One*, September 17, 2018, https://www.defenseone.com/threats/2018/09/congresss-quantum-science-bill-may-not-keep-us-military-ahead-china/151319/; Sandra Erwin, "Pentagon Sees Quantum Computing as Key Weapon for War in Space," *SpaceNews*, July 15, 2018, https://spacenews.com/pentagon-sees-quantum-computing-as-key-weapon-for-war-in-space/; National Quantum Initiative Act, H.R. 6227, 115th Cong., https://www.congress.gov/bill/115th-congress/house-bill/6227; European Union, *Quantum Manifesto*.

[37] Larry Greenemeier, "How Close Are We—Really—to Building a Quantum Computer?" *Scientific American*, May 30, 2018, https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/.

[38] Jon Harper, "Support Growing for Directed Energy Weapons," *National Defense*, May 4, 2018, http://www.nationaldefensemagazine.org/articles/2018/5/4/support-growing-for-directed-energy-weapons; Richard D. Fisher Jr., "China's Progress with Directed Energy Weapons," Testimony before the U.S.-China Economic and Security Review Commission hearing, Washington, DC, February 23, 2017, https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf.

The views expressed in this paper are the authors' and do not necessarily represent those of the organizations with whom they are affiliated.

Admiral Gary Roughead (USN, ret.) is the Robert and Marion Oster Distinguished Military Fellow at the Hoover Institution and co-chair of the National Defense Strategy Commission. He served as chief on naval operations and before that commander of the U.S. Pacific Fleet and Fleet Forces Command. Dr. Ralph Semmel is the director of the Johns Hopkins University Applied Physics Laboratory, the nation's largest university affiliated research center, and Emelia Spencer Probasco is the chief communications officer for the laboratory.

Observations from the Roundtable

By James O. Ellis, Jr. and George P. Shultz, Hoover Institution

When looking at the security environment, we are reminded of President Reagan's approach to dealing with a complex and dangerous world. The first order of business was to be realistic about the world around you. Then you had to be strong in all senses of the term—military, economically, politically, and in national spirit. Finally, as you went out into the world, you had to set your objectives—know what you want—and focus on that agenda. It was a wise, and ultimately successful approach.

Today we see great challenges arising in the security arena but also great opportunities to create a safer, more secure world. We see the emergence of new technologies and the development of new ways of using them for military means. China is adopting these new tools particularly well and devising effective concepts and strategies for their use; Russia is employing internet and communications technologies while also developing certain high-end capabilities; and non-state actors are gaining access to new, increasingly lethal weapons.

More broadly, we recognize that the emergence of new economic centers leads to new technological centers, as in China. And we see the globalization of technology: new and emerging technologies are being developed across borders and across disciplines. The nature of these technologies contributes to their globalization. Some, such as additive manufacturing, democratize production, while effective and creative applications of artificial intelligence (AI) are being developed openly and internationally. We need to understand how these phenomena are changing the face of international security and what they mean for the United States.

At the same time, we can make sure that the United States continues to operate from a position of strength. Fortunately, we have a good foundation. The United States has led the modern world in science, technology, and innovation, and that leadership underpins American economic and military supremacy. U.S. scientists, mathematicians, and engineers excel at fundamental research but also at transforming that research into usable technology, realizing new military capabilities. Our nation owes that advantage to any number of factors, among them an entrepreneurial spirit and culture of innovation, centers of scientific excellence at universities, a conducive business environment, and a productive relationship between the public and private sectors. And the United States also enjoys an expansive network of partners and allies that excel in this arena.

Although challenges to U.S. preeminence have appeared and are chipping away at our technological edge, the emergence of new technologies offers great opportunities for the United States. Revitalizing our national tradition of excellence in the development of critical technologies and their practical applications will contribute to both our national security objectives and our economic prosperity—and to our ability to lead international security efforts.

The emergence of new technologies will not, in itself alone, invariably shape the future. If we recognize the challenges and opportunities before us, we can develop sound strategies to strengthen our own innovation base, we can work with our allies and partners, but also with Russia, China, and other nations, to shape a more stable future.

China and the Indo-Pacific

The United States and China share extensive ties in trade, investment, science, and diplomacy, and citizens of the two countries maintain historically deep personal connections. Overall, this is a relationship with strong mutual benefit. At the same time, the United States engages in competition with China on economic, technological, military, and even ideological fronts. The PRC's integrated information technology strategy, in particular, makes it uniquely capable of disrupting the liberal order championed by the United States and its allies.

Importantly, the nature of these field of competitions is new. Kinetic engagements—what we generally think of when we think of war—are of course central to any military conflict, but, as Admiral Gary Roughead (USN, ret.), Emilia Spencer Probasco, and Ralph Semmel write, information is transforming both the nature of competition and what it means to win in war. U.S. technological innovation and cultural attractiveness has in recent years allowed it to enjoy information dominance, and now the Chinese Communist Party (CCP) has made a national commitment to achieve that same objective.

It is easy to speak about the opportunities presented by technology but another thing to realize them. In the military sphere, China has taken that latter step and embarked on a national effort to take advantage of information technology and control. It is building institutions to coordinate fielding and use of high-tech capabilities, such as the Strategic Support Force, which integrates cyber, space, and electronic warfare operations. It has taken advantage of its status as an emergent and expanding power to invest in leap-over technologies. And the party state mandates civil-military cooperation, forcing a whole-of-nation approach and benefiting from its innovative and entrepreneurial society.

The latter point deserves some attention. As addressed in our October 2018 volume on *China in an Emerging World*, Chinese innovation is not solely state-directed but organic and extensive. China has significant risk tolerance, encouraging rapid and widespread adoption of new technologies. Moreover, U.S. corporations—consider Alphabet/Google—seek to reach global markets, while their Chinese counterparts may have a different set of incentives or trade-offs. The CCP has established legal authority to demand cooperation from private entities.

The CCP and the People's Liberation Army (PLA) have succeeded in the "gray zone." Where U.S. policymakers often view gray zone competition as geographic—the South China Sea, to pick a common example—Chinese authorities understand it as a broader, cross-functional competition. They employ "below-the-line" approaches to competition widely, overlaying physical infrastructure investments with information campaigns, legal maneuvering, coercion, and other applications of influence and power. The fruits of their labors can be seen in the aforementioned South China Sea, where some believe China has created a *fait accompli*.

New information infrastructure and applications put China in a position to extend its influence in telecommunications, information systems, and e-commerce in developing countries and strategically significant locations (including space). China's innovations could end up serving as the infrastructure of the future information society and position China for technological and political advantage should its standards, systems, and policies be adopted widely by others. Its efforts to establish a global foothold in this respect have met some resistance, as can be seen in the ongoing disputes over whether the Chinese telecommunications company, Huawei, should or should not be allowed to supply new 5G networks in the United Kingdom and other U.S. allies.

All told, China employs a comprehensive, national approach to developing, fielding, and employing information technologies, many of which are dual-use—valuable for both civilian and military enterprises. At the same time, it faces some significant structural problems of its own, which may hinder its ability to meet its own expectations: a poor demographic outlook; a slowing economy that is weaker than advertised; and an overly authoritarian government. Moreover, U.S. private organizations still lead in high-tech development, though Chinese firms are close behind and getting closer. What distinguishes the Chinese approach to new technologies—and what deserves further discussion—is the way the PLA is integrating them across all domains of warfare, from undersea to space.

In their paper, Roughead, Probasco, and Semmel consider what might happen if President Xi tried to realize the long-standing CCP goal of reunifying Taiwan. China's investments in information technologies and PLA capabilities, coupled with sophisticated operational concepts, would give it a wealth of tools for forcing the issue. It could put on an impressive show of force, deploying submarines and other naval assets into the Taiwan Strait while test-firing missiles—two well-funded and developed capabilities. At the same time, it could activate an undersea sensor network using unmanned undersea vehicles; disrupt the U.S. GPS system without interrupting the parallel Chinese BeiDou system; conduct a social-media-based information campaign to undermine political will and confidence in the United States; interrupt power supplies in Taiwan and neighboring islands; control global shipping in an out of ports it owns; and so on. The Taiwan scenario is a compelling one, and one that shows the potential of well-integrated technologies and creative strategy and operational plans. And it highlights the importance of specific, high-end technologies to the future of conflict in the Indo-Pacific region:

Artificial Intelligence: For both sides, an important political precondition for conflict is that it would be "quick, decisive, and ultimately deflating to the adversary." Roughead, Probasco, and Semmel write that AI and the autonomous systems it enables, "could affect the entirety of the information life cycle—how we collect it, secure it, manipulate it, defend it, share it, process it, integrate it, and act with it." Artificial intelligence has potential for speeding up the pace of conflicts, both forcing and enabling quicker decision-making and responses. At the same time, it can facilitate coordinated, multidomain operations—both offensive and defensive—and allow control and manipulation of intelligence and information, as in deep fake videos. And AI also enables drone swarms and other advanced autonomous systems.

The history of AI development shows intermittent "AI Springs," during which researchers make meaningful advances for a short period of time before progress plateaus yet again. What we are seeing today may be a fundamentally different scenario, the development of new applications of AI for civil and military purposes. China excels at AI research and applications, generating the most AI-related patents—a crude measure to be sure, but a telling one—and has set up legal and political mechanisms to ensure the PLA and government entities have access to privately-developed technologies.

Cyber: Although not an "emerging" technology, cyber is fundamental to information warfare. It is ubiquitous but vulnerable, so, to quote the Defense Science Board, "defense is a necessary foundation for offense." That means defending military platforms and networks during operations but also protecting intellectual property, supply chains, military networks generally, and personnel information. This takes personnel trained in computing disciplines, and China has an impressive supply of experts coming through the university pipeline. Good defense will become harder for everyone with the arrival of 5G networks, which will create high-visibility targets for the collection, manipulation, and sharing of information. As referenced above, China aspires to develop and define the standards for 5G and to own the infrastructure. If it succeeds, it could wield decisive influence across Eurasia; the feasibility of auditing the security of a communications supply chain is unclear.

Space: Both the U.S. and Chinese militaries rely on space-based assets for information transfer and positioning, navigation, and timing information. Space is central to military operations, to the effective use of precision weapons, and greater still to the functioning of the global economy.

Our space assets were designed for an uncontested environment, which we no longer have. Launch capabilities through competitive public-private partnerships, including for military assets, are an emerging bright spot in U.S. technological capabilities. Nonetheless, last year, China surpassed all other nations in orbital launches, and it has demonstrated significant anti-satellite capabilities. The U.S. government remains unnecessarily tight-lipped about the challenge in this domain. It ought to share more information about it, be more vocal about the challenge, and advocate for what must be done to assure access to such a vital domain.

Others: Other key issues include quantum technologies and electronic warfare (EW) and directed energy. The former qualifies as a true emerging technology—one still in the preliminary stage of development. Though it seems perpetually "20 years away," as the authors note, quantum computing and sensing would accelerate AI, revolutionize sensors, and render public key encryption obsolete, while also introducing incredible opportunities for positive technological advances. EW and directed energy are more narrowly confined to military use than other high-tech tools listed here, but they fall alongside cyber in the continuum of information technologies. Directed energy weapons, for example, may be key to defense against autonomous systems. Both the United States and China are working hard in each of these areas, with China arguably leading the way in EW.

Recommendations

China has undertaken a long-term military modernization and reform program designed to prepare it for an information-based competition. Its navy outnumbers ours and our allies' in the Western Pacific, and the PLA has planned carefully for a potential conflict with us. We would, as the National Defense Strategy Commission warned, struggle to win or maybe even lose a war with the PRC.

But, again, China has significant internal demographic, economic, and political challenges of its own, and this competition is a national one, not merely a military or technological race. Chinese leadership will have to answer some difficult questions about whether they can sustain the current rate of military spending growth and continue to bring new opportunities to their people. From that perspective, the United States is well-positioned. It remains the preeminent power—economically, militarily, and technologically—and our liberal system opens us to vast amounts of human potential. The challenge will be to muster our great national power and competence.

If we narrow our gaze to new technologies, as we have here, we can identify specific steps to take here at home to do just that. To begin with, we should focus more on the speed of practical applications than on revolutionary technologies. That is, think about how best to get new technologies out of the laboratory and into the field quickly and then use them most effectively.

Productive civil-military integration will be key to that effort. As discussed above, the Chinese system mandates effective exchange of technologies and concepts, but the U.S. relationship among government, academia, and industry, which has traditionally powered American innovation, could be stronger still. The national security and defense strategies label this ecosystem as "the national security innovation base" and call for the strengthening and protection of that base; we concur. More broadly, we should focus on bringing public leaders and technologists together, at all ages.

From a strategic perspective, we can support the development of even more intellectual capital. American students now comprise a surprisingly small portion of U.S. STEM graduate programs, and the government struggles to train and retain high-quality civilian talent. Our immigration system should be improved to attract and keep talented people in the United States, and the government can do more to encourage the intellectual development of young experts. Beyond our shores, our allies and partners possess great intellectual capital of their own, multiplying our collective capacity. It will be important to maintain and strengthen them instead and to build public support for them both at home and abroad.

Of course, China's population outnumbers America's, and China enjoys great human, intellectual capital of its own. It is incumbent upon us to recognize reality, to educate the public about this new reality, and to be clearer and more analytical about our national strategies—for example, reconsidering our approach to gray-zone competition. As technologies increase the speed of decision-making and warfare, we should also remain mindful that speed may help on the battlefield, but in strategy it can lead to instability.

The United States enjoys important advantages across the spectrum of technologies and high-end military capabilities and from its network of allies and partners, and its strong, open economy and society. We should strengthen and sustain those pillars of national power, while moving our relationship with China beyond a zero-sum competition. Operating from a position of strength and confidence, the United States can work with the Chinese to build a healthier, more productive relationship.

The European Theater

Turning our eyes across Eurasia, we see a revisionist Russia and a NATO alliance in need of greater political unity. Russia, faced with significant strategic disadvantages of its own—among them poor demographics and a weak economy—knows it cannot match the United States and its European allies across the board. Instead it looks for those areas in which it can compete; in the words of one participant, it seeks "multiple levers against the West." General Philip Breedlove (USAF, ret.) and Margaret Kosal write that Russian development of high-end technologies should not be our primary concern, and our project's earlier assessment of Russia, in *Russia in an Emerging World* (October 2018), concurred. For all of President Putin's rhetoric about the importance of AI, his government has done little to foster a true innovation base.

Russia's "levers against the West" do include some emerging technologies, such as hypersonics and autonomous systems, and we should not lose sight of its development of those capabilities. But for the most part, it focuses on information warfare, certain asymmetric capabilities—such as integrated air defenses and long-range artillery—and nuclear weapons. Arguably, Russia has done the most damage to the West through the former: its cyber-enabled political and information warfare campaigns.

Russia seeks coercive power through information manipulation and control. It exploits political divisions in Europe and the United States to weaken NATO and undermine confidence in Western, democratic systems. The 2016 presidential election may be the most obvious example, but Russia interferes in elections and political processes across Europe as well. Though President Putin's efforts seem opportunistic—targeting divisions or weaknesses as he sees them—the objective is clear: Russia seeks to sow discord and confusion, thereby imposing long-term, significant costs on the West, especially the United States.

To achieve that end, the Kremlin has closed the gap between the military and the rest of government, integrating non-military capabilities into military operations to conduct full-spectrum competition—what we might call a "whole-of-government" approach. It also leverages relevant technologies to support that effort: realizing the discordant potential of social media on the low-end and the value of autonomous systems at the high-end, for example. And its operational concepts are innovative and deadly. Its proxies have used drones to coordinate and target artillery barrages rapidly and to great effect, proving that the ability to employ technology to generate strikes can sometimes trump the size of battalions.

The contrast between the Russian "whole-of-government" approach and the limited U.S. response is striking. It may be derivative to say the United States can do a better job of mobilizing all aspects of national power to the challenge, but it is true. Despite our economic, military, and political advantages—and our close allies in Europe—we have not put up a good stop sign for President Putin. We have relied on economic measures to punish Russia, ignoring the array of other tools at our disposal.

Recommendations

How can the United States bring its vast capacities to bear in the European theater? To begin with, we should maintain our technological lead. Though Russia is not a technological powerhouse, we can achieve more asymmetries through high-tech capabilities. That effort need not be undertaken alone; we should encourage technology transfer and cross-border development with our allies and partners. Sweden's cooperation with NATO in this arena is a good example of broad-scope tech development. Of course, as we have seen before, we must be careful to protect technologies as we go. Bad actors will often target smaller contractors and weaker governments—the weak links in the supply chain—so careful civil-military integration throughout the NATO alliance and its partners will be crucial. But we know that can be done; we can look to Estonia to see how a nation can harden its infrastructure and institutions and master its own destiny.

Taking a broader view, we return to the oft-referenced idea of a more balanced, "whole-of-nation" approach. It bears repeating that the West can do a better job in the information arena and telling the story of U.S. and NATO values and how we operate. We can truthfully promote our ideas and call out bad actors, and we can be less linear in our behavior, employing information operations, but also diplomatic efforts, to get off the defensive.

Of course, such a united effort requires political will and coordination, both at home and throughout the alliance. NATO members have, for four years running, increased their defense spending. They have, as mentioned, bolstered their efforts to cooperate on cyber issues and elements of information warfare. And they have shown firm resolve against Russian aggression, as in the deployments of battlegroups to the Baltic states and Poland. However, the political cohesion of the alliance is not as strong as it could be. If NATO members come closer together again, the alliance will be in even better shape to take on these challenges. As one participant noted: if we cannot build a political narrative of our own, shame on us.

In the 1980s, the leaders of the United States and NATO came together and agreed to deploy Pershing II nuclear missiles in Europe as a response to the Soviet Union's own nuclear deployments and saber-rattling. It required a massive diplomatic effort and a healthy, united alliance, but it turned the tide of the Cold War. It was a non-linear response to the Soviets, a stop sign. We need another stop sign today. A new Pershing moment will likely not be based around nuclear weapons, but it will require renewed American leadership and a revived NATO.

Non-State Actors

Finally, let us turn our attention to non-state actors. Though discussions of how the United States should deal with non-state actors often fall to the tactical or operational levels, T.X. Hammes argues that we ought to look at better strategies. Insurgents, terrorists, and criminals are adopting new, but not cutting-edge, technologies and employing them in innovative ways, including AI-enabled autonomous systems. As those technologies become more accessible, they will give non-state actors the kind of affordable, long-range weapons major powers have generally had to themselves. Counterinsurgency and counterterror operations will become increasingly challenging. U.S. planners will have to change how they think about intervening abroad.

Insurgents generally prefer to employ available and widely used technologies. During the Iraq War, they used such commonplace items as garage openers and then cell phones as detonators for improvised explosive devices. Now, in Syria, we see increasing use of unmanned aircraft—commercial drones. Autonomous aircraft are quickly becoming cheaper and more capable, while task-specific artificial intelligence improves their operations and multiplies their uses. A drone equipped with a camera, for example, can employ high-quality facial or target recognition software—consumer technologies already available to hobbyists—to become a targeted weapon. At the same time, additive manufacturing (3D printing) makes them easier to build or repair in the absence of a dedicated supply chain and may, in the near future, allow inclined parties to mass produce them.

Hammes reviews the various ways in which insurgents or terrorists might use autonomous systems. Coupled with explosively formed penetrators (EFPs), they could target vehicles, disabling or even destroying them. A simple thermite grenade dropped onto fuel or ammunition dumps could ignite a conflagration, as has happened in Ukraine. Drone attacks on a civilian airfield could disrupt air travel, while one on a military airstrip—or resupply depot or convoy—could interrupt logistics.

In sum, these new technologies will allow insurgents and terrorists to target and hunt specific targets. At the most basic level, troops in Iraq and Afghanistan have spent the past decade and a half staring at their feet for hidden IEDs; now the IED can come to them.

Other advantages accrue to insurgents. Drones are no longer dependent on GPS, instead relying on inertial and visual navigation, and non-state actors can locate targets through cheap space access—namely Google Maps and Google Earth. The ability to attack specific targets makes physical infrastructure and public figures more vulnerable, favoring the disaggregated insurgent force and working against the established power.

These technologies exacerbate existing obstacles to effective counterinsurgency operations, but the effectiveness of those efforts have always depended on strategy. As Hammes puts it, nations lose strategically not tactically. When we commit to nation building, we commit to a long-term conflict and a heavy footprint. But as insurgents arm themselves with these new capabilities, they can further exploit that large footprint, targeting U.S. bases, political infrastructure, and the like; it becomes even more challenging and costly to maintain presence and establish general security.

The logical response to an enemy holding static or large formations at risk is to disperse and minimize your footprint. It would seem, then, the best response to a newly-capable insurgency would be first to avoid large, direct interventions in the first place and to harden facilities—overhead protection, for example—as needed. Of course, the former decision is a fundamentally strategic one. At minimum, policymakers and strategists must be attuned to technological changes and adapt their understanding of counterinsurgencies accordingly; we must avoid faulty assumptions in a rapidly changing dynamic.

Conclusion

We return to President Reagan's approach to a changing, complex world. What does the emergence of new technologies mean for international security? How can the United States keep itself in a position of strength? And how can it help stabilize the international order and set the conditions for a more peaceful world?

We recognize that Russia, China, and non-state actors present fundamentally different challenges to the United States, but for each we must deal with the emergence of new capabilities from a strategic perspective. As non-state actors gain access to increasingly capable drones, for example, U.S. military strategists will have to rethink our approach to fighting them and engaging with broken states. Russia, meanwhile, presents a challenge in specific areas, including nuclear weapons, high-end offensive cyber capabilities, and in the low-end technologies of information warfare. The United States and its allies enjoy a much stronger position than Russia, but they ought to develop new, non-linear responses to Russian revanchism and put up a stop sign for Putin. Finally, the most pressing concern is China's military build-up, adversarial behavior, and pursuit of military and commercial applications of AI and other new technologies and standards. The key in the Pacific will be information dominance; from undersea to space, information is transforming the definition of winning.

Emerging technologies give America's competitors new capabilities and transform the character of competition, but they are no less available to us than to others. The key issue is not so much access to these new technologies but their practical application to military capabilities. They are predominantly dual-use technologies, blurring the lines between civilian and military tech development, and are increasingly developed across borders. The key for the United States will be to leverage its vast supply of resources—human, financial, and capital—and continue its long tradition of excellence in technology development and practical innovation.

One area of focus should be the rapid development and fielding of "bleeding-edge" technologies, including AI, hypersonics, metamaterials, and directed energy. We should also improve how we incorporate and employ emerged technologies, such as some task-specific AI, cyber, and electronic warfare. Technologies alone do not mean much for anyone, innovative concepts for how best to use them do. Transforming scientific progress into real capabilities, though, requires both process and cultural adaptation.

As the discussion of China and Indo-Pacific addressed, we should strengthen our education system and better integrate government, academia, and industry. American citizens represent a relatively small portion of the qualified and well-trained technical experts coming out of American schools, and they are the only students allowed to work in classified environments, such as the Pentagon and the defense industry. The military, and the Department of Defense writ large, can do a better job of attracting, training, and retaining talent. The civilian side, for example, should encourage continuing education in its technical experts and strategists, just as the military does. The military, for its part, would be wise to encourage ingenuity in the ranks and allow more creative, bottom-up solutions—put the already innovative minds of the troops to use—though we recognize the attendant security risks and organizational challenges. It could also consider additional ways to allow specialized personnel—software engineers or other tech experts, for example—to rotate into the force as needed.

As the same time, better integrating the public sector with academia and industry will help us those graduates make full use of their talents and renew the system of research, development, and innovation. From our perspective here at Stanford, the gap between Silicon Valley and the Pentagon looks increasingly like a chasm; we can narrow it.

Similarly, we enjoy a unique system of allies and partners. Our European allies lead the world in publication of papers on AI, and our allies and partners in the Indo-Pacific are numerous and capable. We would be wise to remember the value of that system and work more closely on technology development with our allies. The United States too often views military sales and cross-border data exchange through a purely business lens; they are security issues too.

A key aspect of the emerging technologies discussed herein is speed, including the speed of development, yet the government's approach to acquisitions is notoriously slow. The time it takes to develop and field a new capability is crucial and ought to be considered alongside cost and performance metrics. Congress and the administration have expanded the Pentagon's rapid acquisition authorities for the better; flexible acquisition models will help the government reach into non-defense sectors and build better civil-military relationships with industries. Software development, for example, is iterative, which makes it fit poorly within the Pentagon's requirements-driven model. As a note of caution, though, speed is not always a good thing. In matters of national security, sober-minded strategic thinking can trump action. Rapid deployment of a new technology for its own sake will get us nowhere.

Increasing the speed of acquisitions and scope of military capabilities requires more funding, both for the military and other agencies. High-tech research and development come with risks and require significant human and physical capital. Failure is unavoidable but a good thing. And while we pursue these emerging technologies, we recommend also addressing the very real, immediate defense challenges that confront us: significant military readiness shortfall, a shifting conventional balance of power, rogue states, and an assertive China.

Fortunately, new technologies may be disruptive, but they can benefit the U.S. military in meaningful, if mundane, ways, as U.S. Army captain and Stanford PhD candidate Katie Hedgecock explained in her public remarks. They can simplify and reduce the costs of logistics, the lifeblood of operations: AI-enabled predictive maintenance coupled with 3D printing, for example, may soon reduce the logistical tail needed for forward operations. They will likely aid battlefield decision-making, easing the transition towards more dispersed, survivable command and control nodes. And AI may well improve personnel and talent management, reducing administrative burdens and freeing resources for warfighting.

The future of our relationship with China, Russia, and other actors is not foreordained; it will depend on what we do. We can strengthen ourselves at home and recommit to American leadership. But we must also engage with those countries and work with them to build productive relationships. Effective diplomacy can secure our interests, helping, among other things, to prevent military accidents, protect international trade, and support democratic efforts around the globe. Indeed, diplomacy and military strength are inextricably linked and necessary, complementary tools of national power. We have advocated for a "whole-of-country" approach to addressing changing military technologies and capabilities. But it is important to remember that those efforts are carried out in the interests of our diplomatic goals. The best thing we can do for our military is to meet our strategic objectives without having to use it. Diplomacy without strength is weakness, but so too is strength without diplomacy.

George P. Shultz is the Thomas W. and Susan B. Ford distinguished fellow at the Hoover Institution and former secretary of state, treasury, and labor and director of the Office of Management and Budget. Admiral James O. Ellis, Jr. (USN, ret.) is an Annenberg distinguished visiting fellow at the Hoover Institution. He served in the U.S. Navy for 39 years, retiring as commander of U.S. Strategic Command.

About

New and rapid societal and technological changes are complicating governance around the globe and challenging traditional thinking. Demographic changes and migration are having a profound effect as some populations age and shrink while other countries expand. The information and communications revolution is making governance much more difficult and heightening the impact of diversity. Emerging technologies, especially artificial intelligence and automation, are bringing about a new industrial revolution, disrupting workforces and increasing military capabilities of both states and non-state actors. And new means of production such as additive manufacturing and automation are changing how, where, and what we produce. These changes are coming quickly, faster than governments have historically been able to respond.

Led by Hoover Distinguished Fellow George P. Shultz, his Project on Governance in an Emerging New World aims to understand these changes and inform strategies that both address the challenges and take advantage of the opportunities afforded by these dramatic shifts.

The project features a series of papers and events addressing how these changes are affecting democratic processes, the economy, and national security of the United States, and how they are affecting countries and regions, including Russia, China, Europe, Africa, and Latin America. A set of essays by the participants accompanies each event and provides thoughtful analysis of the challenges and opportunities.

Efforts have been made to locate the original sources, determine the current rights holders, and, if needed, obtain reproduction permissions. On verification of any such claims to rights in the articles reproduced in this book, any required corrections or clarifications will be made in subsequent printings/editions. Hoover Institution assumes no responsibility for the persistence or accuracy of URLs for external or third-party Internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Hoover Institution,
Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER
INSTITUTION