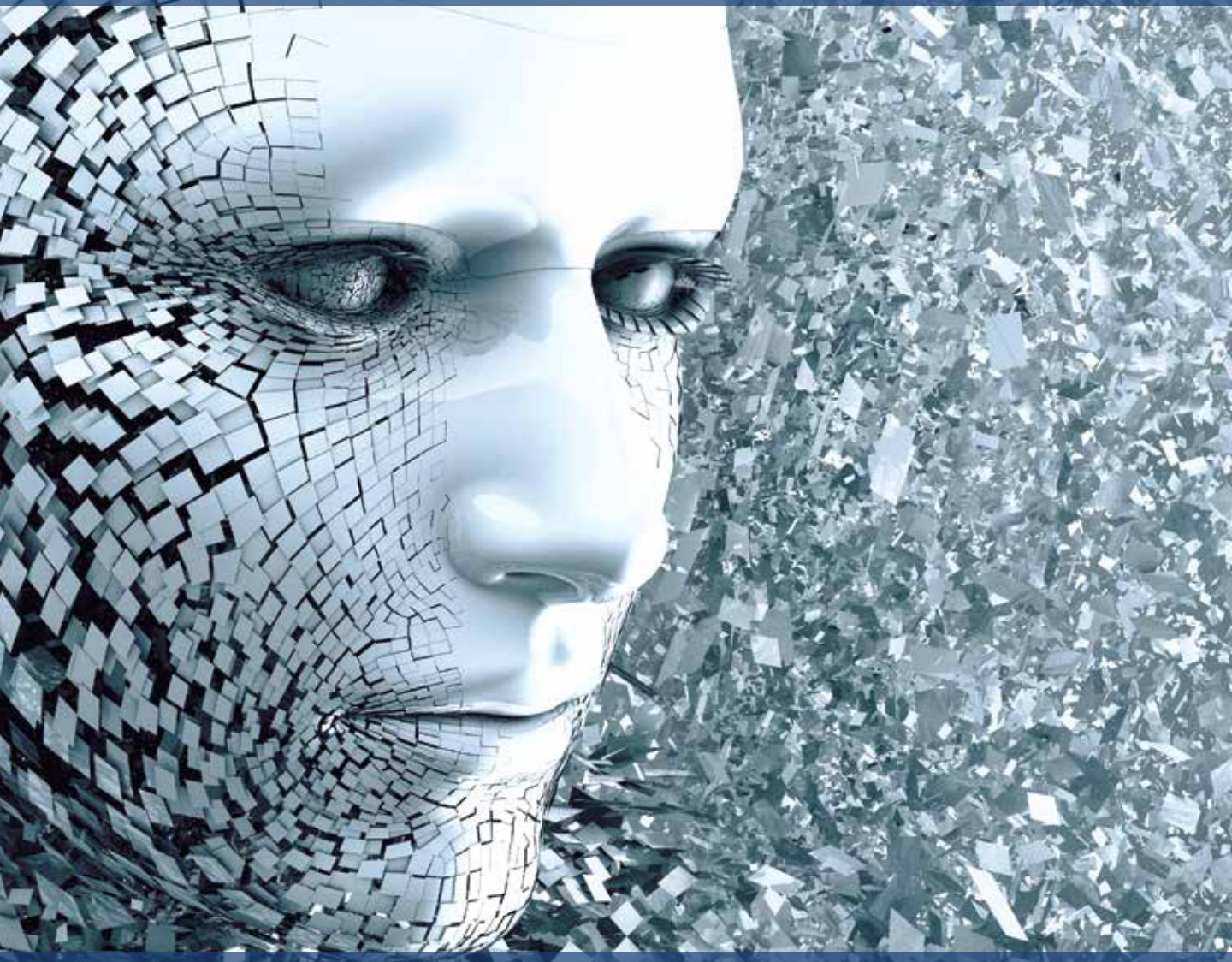
PRISM

VOL. 8, NO. 3 | 2019

SINGULARITY



THE JOURNAL OF COMPLEX OPERATIONS

PRISM
VOL. 8, NO. 3 2019

ISSN 2157-0663

ABOUT

PRISM, the quarterly journal of complex operations published at National Defense University (NDU), aims to illuminate and provoke debate on whole-of-government efforts to conduct reconstruction, stabilization, counterinsurgency, and irregular warfare operations. Since the inaugural issue of *PRISM* in 2010, our readership has expanded to include more than 10,000 officials, servicemen and women, and practitioners from across the diplomatic, defense, and development communities in more than 80 countries.

PRISM is published with support from NDU's Institute for National Strategic Studies (INSS). In 1984, Secretary of Defense Casper Weinberger established INSS within NDU as a focal point for analysis of critical national security policy and defense strategy issues. Today INSS conducts research in support of academic and leadership programs at NDU; provides strategic support to the Secretary of Defense, Chairman of the Joint Chiefs of Staff, combatant commands, and armed services; and engages with the broader national and international security communities.

COMMUNICATIONS

PRISM welcomes unsolicited manuscripts from policymakers, practitioners, and scholars, particularly those that present emerging thought, best practices, or training and education innovations. Publication threshold for articles and critiques varies but is largely determined by topical relevance, continuing education for national and international security professionals, scholarly standards of argumentation, quality of writing, and readability. To help achieve threshold, authors are strongly encouraged to recommend clear solutions or to arm the reader with actionable knowledge.

Our review process can last several months. The *PRISM* editorial staff will contact authors during that timeframe accepting or regretfully rejecting the submission. If the staff is unable to publish a submission within four months of acceptance, *PRISM* will revert publication rights to the author so that they may explore other publication options.

Constructive comments and contributions are important to *PRISM*. We also welcome Letters to the Editor that are exclusive to *PRISM*—we do not publish open letters. The *PRISM* editorial staff will contact authors within two months of submission if they accept the letter for publication.

Potential authors can submit their manuscript for blind peer review at <prism@ndu.edu>. Writing guidelines, tips, and tricks are available at <https://ndupress.ndu.edu/Journals/PRISM/>.

DISCLAIMER

FEATURES

INTERVIEW

BOOK REVIEWS

The evolution and possible weaponization of Cyber Physical Systems will pose significant challenges to the joint force in the emerging global threat environment. (Nicolle Rager Fuller, National Science Foundation)

Cyber Physical Systems
The Coming Singularity

By Marty Trevino

At this moment, a subtle but fundamental technological shift is occurring that is uniting our digital and physical worlds at the deepest architectural and operational levels. This technological shift will alter the global business, government, military and intelligence ecosystems. It is nothing less than a technological singularity and this technology will forever change our world—it is called Cyber Physical Systems (CPS).

This ill understood technological singularity is easily dismissed through cognitive error by strategic decisionmakers who are inundated by cries of technological revolution on a weekly basis. Yet, Silicon Valley visionaries, former National Security Agency (NSA) Senior and Technical Officers, and Tier 1 researchers are comparing this technological shift to a "black swan" event and when assessing its effects, are placing it in the "Unknown / Unknown" category of former Secretary of Defense Donald Rumsfeld's quadradic event characterization schema.[1]

Cyber Physical Systems are at the center of the unification of what have always been distinct physical and virtual worlds. And while the convergence of our physical and virtual worlds is not conceptually new, it is the capability which CPS possess that creates one of the greatest intellectual and technical challenges of our time. Cyber Physical Systems are creating "open systems" able to dynamically reconfigure, reorganize and operate in closed loops with often full computational and communication capability. Machine Learning can be fully integrated within a CPS network and this will soon be followed by partial, and eventually full, Artificial Intelligence—often without the ability of humans to observe the ongoing processes of the system. Cyber Physical Systems are at times even composed of unconventional computational and physical substrates such as Bio, Nano, and Chemical. It is the convergence and morphing of the physical and cyber worlds into multi-agent, intelligent CPS that constitutes nothing less than the technological singularity of our time.

Dr. Marty Trevino works for Fortinet in the office of the CISO as the Senior Director of Security Strategy. He previously served as the Technical Director of Mission Analytics for the National Security Agency of the United States.

Tech Hype and Buzzwords or the Unknown/Unknown

No industry enjoys creating hype more than the technology industry. Every new mobile App, computer program, algorithm, machine learning construct, etc. is dubbed as revolutionary and destined to change the world. The reality is that very little of this hype is accurate; but this does not violate the premise that "black swans" do exist and when they are discovered, they are highly impactful. CPS is today not only highly impactful and seemingly improbable; but in the framing of Rumsfeld, CPS also falls into the Unknown / Unknown category. Simply put, we ignore this technological shift at our peril and open the door to our adversaries who do not ignore this shift.

The fact that we are entering a CPS and Internet of Things (IoT) dominated world is beyond debate. That we do not have the level of understanding required regarding the effects of CPS on the world is also beyond debate. Nor do we have a clearly defined way of attaining the necessary level of understanding required to embark upon military and intelligence operations in foreign cyber space dominated by these systems. These realities present both strategic challenges and opportunities. Attaining the level of understanding of CPS to enable complex operations with designed effects is this generation's equivalent of breaking Enigma; and the strategic implications of doing so are equally great.

Defining and Characterizing Cyber Physical Systems (CPS)

In 2013, a consortium of European experts from France, Germany, Italy, Sweden, the UK, and other nations came together with the main objective of expanding European competence in embedded mobile and the network controls of the evolving class of unionized systems.[2] They called themselves CyPhERS and they set out to define, conceptualize and even model one of the greatest intellectual challenges of our time—the concatenation of the virtual and physical worlds into what has become known as Cyber Physical Systems (CPS).

Cyber Physical Systems represent the coupling of two distinct worlds and their subsets to include: industrial and operational technology, building automation, the Internet of Things (IoT), high speed connectivity (4G and soon to be 5G), cloud and machine learning (ML), all made supremely effective with feedback loops and within cutting edge new architectures. The term "cyber-physical systems" is generally credited to Helen Gill, Program Director for Computer and Network Systems at the National Science Foundation. Gill coined the term somewhere around the year 2006 to characterize the intersection of the physical and cyber worlds. Cengarle et al., notes that CPS is subject to numerous interpretations depending upon the individual lens through which the technology is viewed. The deep penetration of electronics, sensors, and software into every aspect of modern life is referred to in unique nomenclature by the varying communities which are served by those advances. Some of these include: IoT, the 4th Industrial Revolution, Smart Cities, Home Automation, Digital Medicine, etc. The CyPhERS group realized that an expanded view, and thus definitions, of those systems were necessary based on the perceived disruptive potential of multi-agent, intelligent Cyber Physical Systems.[3]

The National Science Foundation provides a base definition for CPS that is widely accepted today:

> *A Cyber Physical System is a mechanism that is controlled or monitored by computer-based algorithms, and tightly integrated with the Internet and its users. CPS systems tightly intertwine the physical and software components, each operating on different spatial and temporal scales, while exhibiting multiple and distinct behavioral modalities.*

This dynamic and complex interaction is agile, and changes based on the context."[4]

Cyber Physical Systems will encompass the entire spectrum of technical systems from tiny to massive in scope and size. Torngren et. al., more over characterize CPS as "inherently multidisciplinary and multitechnological, and relevant across vastly different domains, with multiple socio-technical implications."[5] The strategic implications of this technological shift must be made clear for U.S. military and intelligence operations, in particular at the nation state level where understood mastery of this tradecraft is in itself a deterrent to adversaries.

A Dependent Relationship

The conceptual integration of the physical and cyber domains is not new. It is the scale, multi-agent nature, system intelligence level of integration, and the cross cutting of domains which characterizes Cyber Physical Devices that is both novel and relevant. In conceptualizing what constitutes CPS, and thus what will eventually engender itself in every physical and virtual ecosystem, it is important to note that CPS is the result of a dependent relationship between the Core, Endpoint, Connectivity, and Cloud. CPS are not any single piece of technology; rather the complex integration of devices and architectures made possible by the explosion in Endpoint devices, increases in Connectivity speeds, and the expansion of Cloud capabilities to, at times, include High Performance Computing and embedded / native Machine Learning. CPS is thus networking at multiple and extreme scales, and multiple temporal and spatial scales—at times simultaneously.

Initially triggered by the marriage of Industrial and Operational Technology, CPS now consumes Building Automation (BA) and is enmeshed with the Internet of Things (IoT). Critical to understanding the opportunities and threats of CPS is that when these technologies are combined, they constitute something infinitely more capable than the individual parts.

Cyber Physical Systems (CPS) and the Internet of Things (IoT)

When discussing Cyber Physical Systems, often the first question to arise is how CPS differs from the much talked about Internet of Things or IoT? Is CPS simply hype or an alternative nomenclature for the IoT? The answer is "no." The differences between CPS and the IoT are significant and important to understand.

The Internet of Things (IoT) refers to the massively expanding number of physical devices that feature an IP address enabling internet connectivity and thus, communication between devices and larger systems. These devices range from home speakers to appliances to thermostats. Sedlar et al. state that the "Devices classified as IoT devices are typically connectivity-centric, advocating the best-effort nature of the internet itself, while computation is secondary and, in many cases, minimal."[6] Cyber Physical Systems differ greatly in that they "use shared knowledge and information obtained from sensors to independently control physical devices and processes in a closed loop."[7]

Cyber Physical Systems are defined by highly integrated computation networks, closed loops, and physical processes. CPS can have multiple temporal and spatial scales, as well as be networked at extreme scales. Cyber Physical Systems are multi-agent and often intelligent, with the ability to dynamically reconfigure and reorganize. The result of these combined characteristics is high degrees of automation, and capabilities far exceeding simple communication and the simple nature of IoT devices. CPS is also now perceived as being a primary vector for the IoT to connect with higher order functions. It is this dynamic integration and connection of disparate devices and systems that present tremendous opportunity for both U.S. advocates and adversaries.

Next Generation Analytics—Understanding and Common Operating Pictures

It is written in the Old Testament that King Solomon went to God and asked to be the wisest of all kings. God granted his wish by giving him "understanding." The advancement of CPS and the capabilities they bring presents massive technical and non-technical challenges from the lens of understanding. Among the most easily constructed approaches to developing an understanding or "internal model" from a neuroscience perspective is a deconstructivism-based approach. A deconstructivism approach can be taken in framing this challenge to begin with defensive challenges and offensive opportunities. This framing can then be extended into military networks, kinetic and non-kinetic operations, denial of intent, and the deriving of other effects in the eco-system. Yet, this sort of endeavor, while useful, fails to incorporate a decisionmaker's best asset—Advanced Visual Analytics.

The importance of Visual Analytics to inform common operating pictures and internal models of strategic decisionmakers is widely recognized in the U.S. military and Intelligence Community. Few decisionmakers are not interested in "seeing the data." But seeing the data at meaningful levels of analysis around the IoT and CPS is no simple endeavor. The sheer size of the IoT and complexity of CPS fuels the problems associated with analytics at scale. The problem of analytics at massive scale encompasses both technological challenges and higher order human functions.

Visualizing millions of CPS and IoT devices in a way that informs and facilitates strategic decision-making is a massive challenge for technical experts. At the highest level of analysis this challenge is not new; Uber, Facebook, Twitter, and Google track the movement, activity, and use of millions of devices in near real-time. The challenge becomes fully exposed when altering the use cases to those of a military and intelligence nature. In each of these cases / domains, how to visualize massive amounts of data in a way that underpins human decision cycles with time as a principle variable in the equations remains unsolved. The element of time as a variable cannot be understated, as with each passing minute the number of devices and actions performed increases in a power curve distribution fashion. The reality of scale and time in relation to temporal opportunities and strategic understanding of a dynamic ecosystem opens the door to mandatory discussions of Machine Learning and fully automated decision-making. And yet, the notion of eliminating humans from the decision loops is strongly rejected by those with decision authority today in virtually every domain. Decision cycles or OODA loops (observe–orient–decide–act), as they are commonly referred to, remain a human-centric process informed by data, analytics, and visualizations. Unfortunately, to believe that human beings will be able to make sense of trillions of actions over periods of time and make accurate, timely decisions can be likened to attempting to build a new Maginot Line in an age of precision weapons; advanced analytics and Machine Learning are the keys to building capability to "sense make" in a world dominated by the IoT and Cyber Physical Systems.

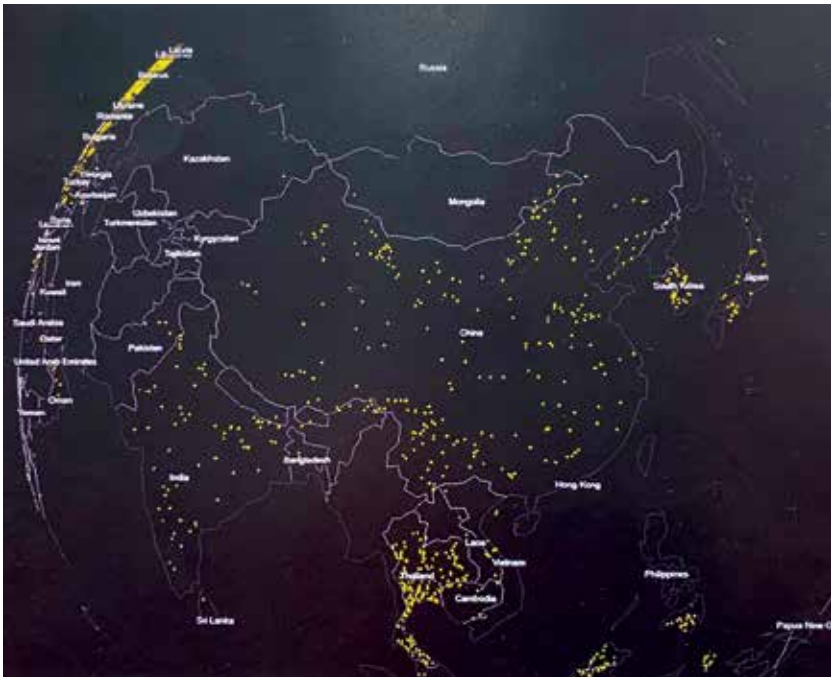
To understand the necessity of developing the next generation object visualization and incorporating Machine Learning (ML and eventually Artificial Intelligence) into the decision process, it is useful to examine a set of current state-of-the-art network visualizations. Consider the visualizations in figures 1-3 to represent both CPS networks and clusters of IoT devices related to those CPS networks across a nation state. Each dot on the map represents a network of no less than 100 CPS for a single industry. In this case, we will consider Oil and Gas facilities at a single point in time to be the target set. The relatively few "dots" reinforces the belief that as an individual or team of people, the target set can be

understood. At this level of analysis, the ability to dynamically "drill down" into the clusters is possible by human analysts and a dedicated team of "experts" could likely glean goodness out of the data.

In this second view (Fig. 2), another single target set of critical infrastructure is visualized. And while the number of networks has increased, as has the dispersion across the nation state (both present challenges from a targeting perspective), size and scale are not insurmountable. Meaningful analysis can still be done in both automated and manual methods and strategic decision informed. The issue is that neither of these views (CPS networks) exists in isolation and the associated IoT devices are not yet shown. To target these networks, one must show contextual networks of CPS systems and affiliated IoT devices.

The final illustration (Fig. 3) is an accurate and complete visualization of both CPS networks and IoT clusters of 10,000 devices or more.

Figure 1. CPS Networks and IoT Clusters—View 1.



Source: Illustration generated by author

Figure 2. CPS Networks and IoT Clusters—View 2.

Source: Illustration generated by author

Figure 3. CPS Networks and IoT Clusters—View 3.

Source: Illustration generated by author

When assessing this level of information density, the human brain is likely to default to a "prone to error" System 1, and these errors have cost U.S. intelligence officers and military commanders dearly across the many wars fought by American warriors. Yet, it is precisely this density of objects that must be dealt with in all future scenarios. In this visualization rendering, only simple presence was considered, device behavior (features) was omitted and time was held to one minute. If we are to capture 100 features from these networks multiplied by the number of devices and networks over a 24-hour period, the complexity challenge becomes clear. Simple decomposition approaches and manual analysis undertaken by even legions of smart people will no longer suffice.

We stand at the event horizon of a technological singularity that, if we are to be "left of boom," an entirely new generation of visual analytics and applications of Machine Learning will be required to inform and perform strategic decisionmaking at speed and scale.

Next Generation Analytics and High Dimensional Space

Military commanders and senior intelligence officers have been quick to realize that advanced analytics are among the keys to situational awareness and successful operations. This truism will only become increasingly obvious as CPS and the IoT mature. Next generation analytics will provide strategic advantages at all levels, but will

fundamentally underpin creative decision processes and higher order human decision functions, such as the weighing of risk and sequencing of kinetic operations. Among the promising and novel approaches to next generation visual analytics is the use of Object Based Analysis (OBA), High Dimensional Space (HDS), and High-Performance Computing (HPC). In considering devices and even networks as objects, features association becomes a powerful tool enabling rich contextual information to be associated with a core object. Adopting this approach enables the creation of unique visualizations designed to capture the inherently dynamic nature of the network and allow the user to interact with the data in ways fundamentally different than what is possible with two dimensional graphs / charts.

Machine Learning, in its various forms, can be unleashed on these data sets with correlations, relationships, and actionable opportunities discovered at speed and scale. These insights can also inform decisionmaking at all levels, but with an emphasis on strategic decisionmaking, as this is fundamentally a creative process in the human brain. It is believed that the outcome can be a new level of understanding for senior commanders, as well as fully automated decision authority for the coming generation of Artificial Intelligence.

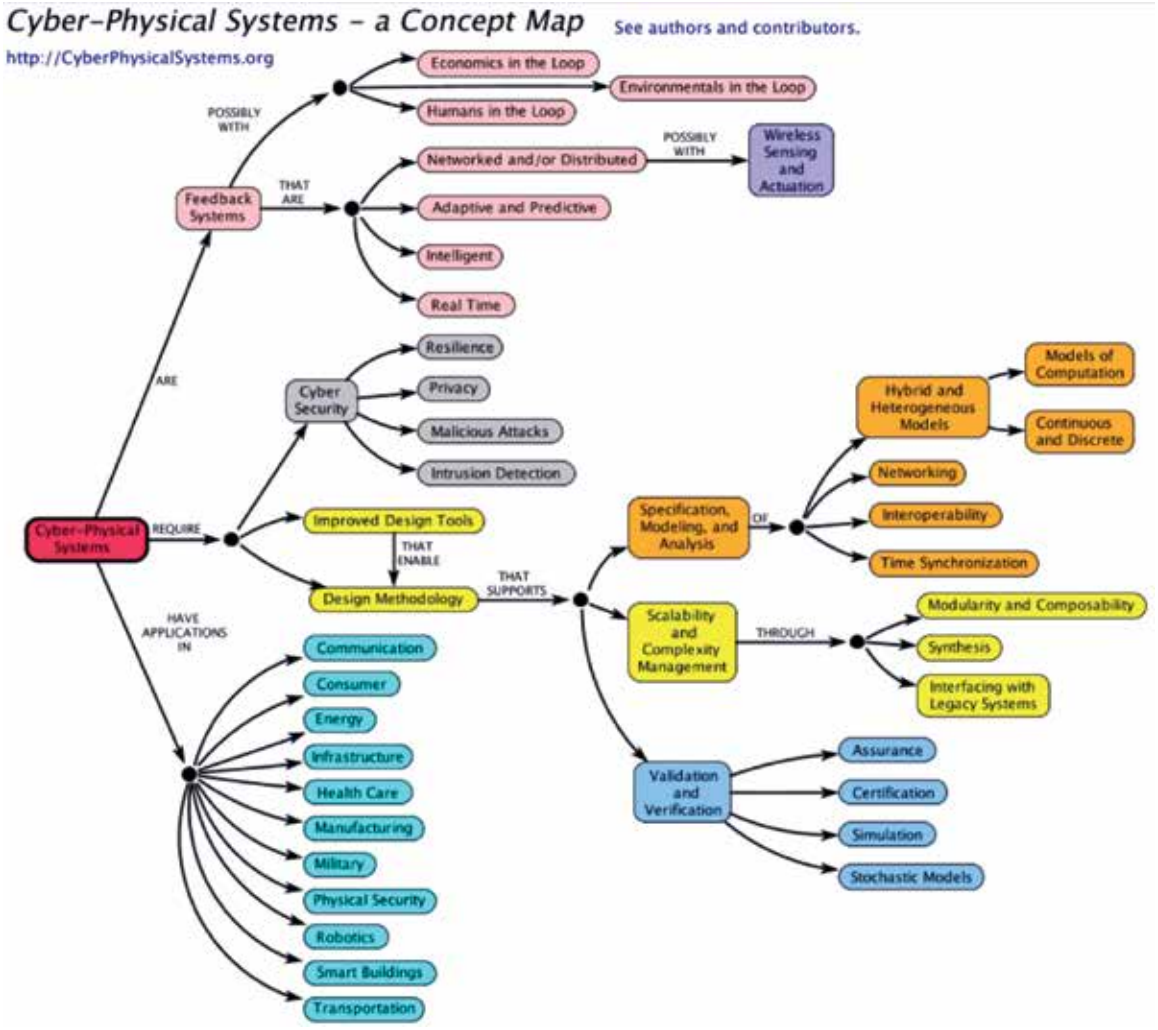
In the most advanced analytic environments, it is possible to stand in the cluster and interact with the visualization in three dimensions by touch and natural language voice processing. The precise benefits of this are currently unknown; but from the lens of the neuroscience of decisionmaking, the possibility to impact the Cortex, Visual Cortex, the Thalamus and hence the formulation of the Internal Model itself is promising. It is possible that even the Amygdala, which plays a decisive role in memory creation, and its ability to override other areas of brain function in moments of extreme danger may be influenced by interacting with data over time in HDS. A theorized outcome would be the creation of "richer" memories also serving to influence the Internal Model for dealing with future high-risk events. Thus, both the technical aspects of analytics at scale and the human brain's ability to process data and make decisions are components in the next generation of visual analytics. To the winner of this race goes the high ground of understanding in rapidly evolving nation state level actions in cyber and any kinetic conflict.

Conceptualizing a CPS / IoT Ecosystem

Attempting to conceptualize a tightly integrated physical and cyber world while it is rapidly evolving can be likened to building an airplane in flight. And while this is not a new conundrum, it has been made markedly more difficult due to scale, speed of development and deployment, as well as the attributes of CPS. Accurately conceptualizing or "framing" the evolving Cyber Physical, or CyPhy, world we must operate within is perhaps the most difficult technical and intellectual endeavor of our time.[8] This intellectually "deep" undertaking is easily dismissed by those in leadership positions as a task to be left to others as "more pressing things" must be attended to. And while there is some truth to this perception, it also can engender the unintended outcome of allowing old Internal Models of the ecosystem to remain intact in the face of a rapidly developing environment; thus, promoting decisions not based on the latest understanding. This tendency to avoid the intellectually deep and difficult foundational work is compounded by the uniqueness of the military and intelligence communities' Use Cases.

The default of many leaders has been to simply adopt frameworks composed by commercial industry or academics. And while this approach can certainly begin the process of framing, from a military and intelligence perspective, it can only be the initial step of developing the required level of understanding.

Figure 4. Cyber–Physical Systems, a Concept Map.



Source: The Ptolemy Project, UC-Berkley, available at <https://ptolemy.berkeley.edu/projects/cps/>.

More robust frameworks have risen out of academic institutions and think tanks. Some of these frameworks have attempted to specifically isolate the component and function relationships of CyPhy. These maps are considerably more useful in illustrating simplistic relationships and the potential interaction of devices and closed loop systems. Yet, even the most robust of these is woefully simplistic in the face of the complex Use Cases of the U.S. military and intelligence services.

At its core, virtually all military and intelligence planning is action oriented. Thus, seeking out existing frameworks which can underpin action can expedite the framing process. In 2010, the McKinsey Institute created a simple, but effective framing of IoT devices which also has application to CPS. This unique stratification is another high level, but useful step in creating a complex framework to underpin operations.

Considerably more work is needed to create the required level of understanding of the singularity we

Figure 5. IoT Device Application Framework .

Information and analysis			Automation and control		
1 Tracking behavior	**2 Enhanced situational awareness**	**3 Sensor-driven decision analytics**	**1 Process optimization**	**2 Optimized resource consumption**	**3 Complex autonomous systems**
Monitoring the behavior of persons, things, or data through space and time	Achieving real-time awareness of physical environment	Assisting human decision making through deep analysis and data visualization	Automated control of closed (self-contained) systems	Control of consumption to optimize resource use across network	Automated control in open environments with great uncertainty
Examples: Presence-based advertising and payments based on locations of consumers	Example: Sniper detection using direction of sound to locate shooters	Examples: Oil field site planning with 3D visualization and simulation	Examples: Maximization of lime kiln throughtout via wireless sensors	Examples: Smart meters and energy grids that match loads and generation capacity in order to lower costs	Examples: Colision avoidance systems to sense objects and automatically apply brake
Inventory and supply chain monitoring and management		Continuous monitoring of chronic diseases to help doctors determine best treatments	Continuous, precise adjustments in manufacturing lines	Data-center management to optimize energy, storage, and processor utilization	Clean up of hazardous materials through the use of swarms of robots

Source: *McKinsey & Company, "The Interntet of Things," McKinsey Quarterly (March 2010), available at* <https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things>.

now face. It is no doubt that more robust frameworks exist at the classified levels and should be sought out through the appropriate channels. It is useful to revisit the wisdom of Albert Einstein who is quoted to have said—"If I had an hour to solve a problem, I'd spend 55 minutes thinking about the problem and five minutes thinking about solutions."

Technological Advances and Implications for U.S. Forces

The operationalization of Cyber Physical Systems on a global scale presents a duality which has few intellectual and conceptualization parallels in today's technical world. CPS also represents one of the greatest opportunities for the U.S. military and intelligence services to create ecosystem effects through non-kinetic operations. These effects can range from influencing foreign decisionmaking to denying an adversary the ability to operate and/or sustain operations against U.S. forces world-wide.

In conceptualizing the possibilities for affecting adversary ecosystems, a principle consideration is that the United States and Europe are leading in the deployment of CPS. Thus, it is possible to evaluate these deployments from a "strengths, weaknesses, opportunities and threats (SWOT)" perspective, and mirror anticipated deployments by our adversaries (understanding of course the differences in Russian or Chinese power grids as an example).

This type of analysis is not new and can simply be applied to CPS development into the kinetic realm. An example of anticipated CPS development

in the kinetic realm can be found in the coupling of high-speed encrypted connections linking multiple platforms. The F–35 Joint Strike Fighter is designed to receive direct data feeds from on station Global Hawks, interpret this data and transmit targeting and prioritization of targets to missile-carrying F–15, F–16 and F–18s. The result of this tight integration through CPS is to enable precise adversarial prioritization and targeting at speed and scale in high-end conflicts. Foreign nations, such as India, have fully integrated high-speed data links in their fighter force. Indian Sukhoi (SU)–30 MK 2s are frequently observed communicating through these modes. This falls short of a full CPS system, but clearly highlights the development path (which mirrors the U.S. path) which will be taken. This understanding should not be squandered, and analysis performed through both SWOT capability and progression lenses.

In the future, CPS will enable the full automation of robotic systems with wide ranging kinetic capability. One often discussed example is swarm bots with full ranging mission parameters. These include bots designed to confuse adversary targeting systems, while dedicated attack units eliminate enemy units. All of this will be done at cyber speed and on a global scale, with humans in and out of the loop. Both the military and the intelligence community will benefit from the applications and/or compositions of new physical substrates such as Smartdust. Smartdust represents novel applications of micro-electromechanical and even biological systems such as sensors, as well as intelligent bots to detect a wide array of inputs and outputs. Smartdust can be distributed over an area to detect prescribed environmental elements—temperature, light, vibration, etc. usually through radio-frequency identification. Initial tests have been highly successful, thus opening the way to further innovation in this field potentially providing novel vectors to pinpoint situational awareness to U.S. forces or intelligence operations.

CPS are rapidly penetrating and will eventually permeate all military and critical infrastructure verticals of every country. Understanding the deep penetration of CPS into these domains is critical to the success of U.S. forces. It is always preferable to deny the adversary the ability to operate or effectively engage in kinetic operations versus engaging in combat operations with a well-prepared and capable enemy.

Simply put, U.S. forces face an endless set of scenarios in which an infinite number of small and separate systems can work in cooperation to achieve much larger military and intelligence objectives.[9]

CPS Analytics and the Art of the Possible

Advanced analytics provide strategic advantages that are difficult to counter in both the military and intelligence domains. It is an understatement to say that there is significant interest in what next generation analytics will look like and do for decisionmakers. Yet, there is a massive misconception as to the future of cyber (CPS and IoT) analytics which stems from purist thinking in the technical realms and misconceptions in the minds of senior decisionmakers. The question, "what will drive next generation analytics?" is likely to generate several permutations of the same set of bullet points. The list of concerns ranges from the "quality of the data," "trust in the data," "data precision," "speed of analysis," "eliminating bias in the algorithms," "story-telling of the data," "good dashboard design," "data" density ratios," etc. And while all of these are important, they all pale in importance to the neuroscience of decisionmaking. There are two scientific dimensions of decisionmaking which are not considered today but will be addressed two generations from today; these are the Umwelt and the Internal Model.

The Umwelt is the spectrum of information which a living being can sense and process.[10] The Umwelt represents the biological foundations at the

epicenter of both communication and understanding in all animals.[11] For a Tick, the Umwelt consists of the ability to detect heat and body odor, for the Eco Locating Bat, its world is largely constructed out of its ability to sense air compression waves. Humans have a variety of senses; but we are still severely limited in what we can sense – despite the belief that we see everything. Yet, our highly capable human brain can learn to utilize new senses and will in fact form new neural paths if necessary, to interpret these signals. These new information streams are then incorporated into our decision cycles and the formulation of our Internal Model of what constitutes the ecosystem we exist / operate within. It is here that the neuroscience of decisionmaking holds the key to next generation analytics and improved strategic decisionmaking versus improving data precision or designing better dashboards. Next generation analytics will not be better data or colors on a dashboard; but rather it will be augmented sensory sensation and individually centric Artificial Intelligence. Today, work is underway to develop wearable devices which can translate data into modulated pulses to be felt by the individual wearing the device. Next generation analytics will be "felt" as well as seen and the human brain will unconsciously know when "something is wrong" or "right." Augmented sensory sensation, coupled with Artificial Intelligence (AI), is the next generation high ground of analytics for U.S. military commanders and intelligence officers as they engage in a never-ending battle of wits with our adversaries.PRISM

Notes

[1] Taleb Nassim, *The Black Swan: Second Edition: The Impact of the Highly Improbable 2nd ed.* (New York: Random House Publishing Group, 2010).

[2] CyPhERS, "D6.1 +2—Integrated CPS Research Agenda and Recommendations for Action," 2015, available at <http://ww.cyphers.eu/>.

[3] M. Törngren, "Characterization, Analysis, and Recommendations for Exploiting the Opportunities of Cyber-Physical Systems," *Cyber Physical Systems: Foundations, Principles and Applications*, ed. Houbing Song et al. (San Diego, California: Elsevier Academic Publishing, 2016).

[4] National Science Foundation, "Cyber-Physical Systems Program Soliciation NSF-1015," 2010, available at <https://www.nsf.gov/pubs/2010/nsf10515/nsfl10515.htm>.

[5] Törngren, 4.

[6] Urban Sedlar et al., "Big Data Analysis and Cyber-Physical Systems,"*Cyber-Physical Systems, a Computational Perspective*, ed. Gaddadevara Matt Siddesh et al. (New York: Taylor and Francis Group, 2016).

[7] Aaron D. Ames, Paulo Tabuado, and Shankar Sastry, "On the Stability of Zeno Equilibria," Lecture Notes in Computer Science Series, Vol. 3927, "International Workshop on Hybrid Systems Computation and Control, 2006," as referenced in "The Internet of Things," McKinsey Quarterly, October 2010, available at <https://www.mckinsey.com/industries/high-teck/our-insights/the-internet-of-things>.

[8] The term "CyPhy" is credited to Phil Quade, former NSA Cyber Task Force Director and current Fortinet® Chief Information Security Officer.

[9] Daniel Khaneman, *Thinking Fast and Thinking Slow, 1st ed.* (New York, NY. Farrar, Straus and Giroux, 2011).

[10] Umwelt loosely translates to English as the "Surrounding World".

[11] Thomas A. Sebeok, "Contributions to the Doctrine of Signs," *Studies in Semiotics Series*, Vol. 5 (Bloomington, Indiana: Indiana University Press and The Peter de Ridder Press, 1976).

"Every critical infrastructure system in the United States, including that of the USG, depends on commercial telecommunications infrastructure" (from this article)

The Worst Possible Day
U.S. Telecommunications and Huawei

By Thomas Donahue

As a global power, the United States must be able to sustain military forces and project power anywhere in the world, even in the face of resistance from a sophisticated adversary with the ability to infiltrate or disrupt telecommunications and other critical infrastructure within the United States, in space, under the ocean, and in other regions of the world. Policy must consider the worst possible day, not the routine day.[1]

The emergence of the Chinese company Huawei as a leading provider of integrated telecommunications systems is seen as such a security threat that the U.S. Government (USG) has sought to raise barriers to the use of the company's technology in U.S. infrastructure, and even threatened long-standing intelligence sharing arrangements with the nation's closest allies who choose to use less expensive Chinese technology.[2]

While arguably helpful in the short term, the USG must confront the basic problem of whether an acceptable alternative must be based in the United States, and whether the U.S. Government should support even a foreign champion with foreign, trade, and industrial policies to promote a viable global competitor to Huawei. As was done in the wake of initial successes by the Soviet space program, the United States should consider whether its strategic role as a global power requires increased government investment in research, industrial capacity, and programs with specific objectives comparable in scale to the U.S. space program of the 1960s.[3]

This article considers how the United States fell into this dilemma, how the government has assisted infrastructure development in the past, and options for how the USG—in partnership with allies and the private sector—might be able to promote competition in the global market place with a view toward enhancing the resilience of national security communications and critical infrastructure.

Opening Gambit

Telecommunications is both a homeland security and a national security issue because the entire economy depends on a shared, interoperable infrastructure, and because many national security communications ride on top of commercial infrastructure both in the United States and abroad.[4] Nonetheless, the United States generally considers free market solutions as more effective and agile, particularly when it comes to consumer products, even when that means foreign companies dominate a technology market. Even when the government is involved in the creation of a technology, privatization is the preferred outcome, as occurred with the

The author is a former Senior Director for Cyber Operations on the U.S. National Security Council Staff.

internet.[5] The business of integrated telecommunications equipment, however, is not a "consumer" issue; it is about systems used by critical infrastructure. In addition, the business of integrated telecommunications equipment is not a "free marketplace" in the usual consumer sense because the multi-decade timelines for investing in national infrastructures inevitably create cyclic demands as carriers seek to recover their capital expenditure investments and manage financing of these procurements.[6]

The United States, in the wake of a major economic downturn in 2001–02, made "free market" decisions by allowing U.S. industry to succumb to global market forces even as China's companies, Huawei and ZTE, began to emerge in global markets. Now the United States finds itself struggling to control a national security issue without the usual means to compete, namely its own industry.

Despite U.S. efforts to create a more diverse market of telecommunications service providers, the trend for equipment manufacturing has been toward reconsolidation to achieve economies of scale.[7] Market consolidation during the past 15 years has reduced the global telecommunications equipment integrator market to primarily Finland's Nokia, Sweden's Ericsson, China's Huawei and ZTE, and South Korea's Samsung (all but Huawei are publicly traded).[8] The United States now mostly depends on Nokia and Ericsson, with a smattering of Huawei deployments in low-density rural areas (the Rural Wireless Association in December 2018 told the FCC that 25 percent of its members use Huawei equipment).[9] Nokia and Ericsson in recent years have been financially shaky, with debt bonds emerging from junk bond status in 2017 only to lowest-grade investment status in 2018 and 2019, and both companies have suffered negative net income most quarters since the beginning of 2017.[10] Nokia suffered a significant downturn in the stock market after announcing that it would not meet its original growth targets in 2020 and would not be paying dividends in order to help fund development costs.[11]

According to industry market research, Huawei's global market share (including China) for service provider equipment is now greater than that of Ericsson and Nokia combined.[12] As of 2016, Huawei reportedly supplied more than half of the 537 "fourth generation" (4G) mobile networks globally and 59 of the 90 4.5G networks, an intermediate step before 5G.[13] European providers use Nokia and Ericsson equipment but increasingly have turned to Huawei for better prices and "advanced" capabilities that are ready to deploy.[14] The Dutch telecommunications carrier in April 2019 cited a 60 percent price advantage when choosing Huawei.[15] More than half of Huawei's 5G contracts as of July 2019 were in Europe.[16]

This proliferation of Chinese technology is further enabled by Chinese telecommunications service providers working together with other Chinese industries and cities to develop 5G applications within China and offering to build 5G infrastructure for other countries as part of the broader investment Beijing offers under its Belt and Road Initiative.[17] As part of this overall effort, Huawei seeks to dominate the application of 5G for the "Internet of Things"—used in infrastructure and manufacturing—through technology development and the setting of international standards.[18]

Can't We Just Keep Huawei Out of the United States?

U.S. concerns with Chinese telecommunications companies—especially the more successful Huawei—are not new. The USG for years has sought to limit the proliferation of telecommunications equipment manufactured by China's Huawei largely on the grounds that Huawei enables espionage for China's security services.[19] The U.S. Congress released a report on the threat posed by Chinese telecommunications manufactured equipment in 2012.[20] Reports in 2019 from British and U.S. cybersecurity

experts have cited a high degree of risk from a large number of security vulnerabilities well in excess of current industry norms.[21] The African Union in May 2019 renewed its partnerships with Huawei on a range of technologies, from broadband and cloud computing to 5G and artificial intelligence, despite accusations in the media that China used Huawei equipment during a period of five years to steal data from the Union's headquarters in Addis Ababa (construction of which was funded by Beijing).[22]

President Trump in May 2019 issued an Executive Order on supply chains and ordered the placement of non-U.S. affiliates of Huawei on the Commerce Department's Entity List.[23] In addition, Section 889 of the *Fiscal Year 2019 National Defense Authorization Act* began to take effect in August 2019. This bill prohibits federal agencies from using "covered" entities or their subsidiaries and affiliates, including Huawei and ZTE.[24] The bill prohibits federal contracts with companies that use covered entities as of August 2020. The actual impact of these recent policies will not be fully determined until rules and regulations are put in place; however, such impacts may be blunted significantly as part of a broader trade agreement.[25] Other proposed bills call for promoting the development of 5G industry and for ensuring the security of 5G and future mobile telecommunications systems and infrastructure within the United States.[26]

The exclusion policy has the potential to prevent further Chinese deployments within the United States but does not solve the longer-term problem of ensuring trusted communications infrastructure on a global basis for the United States or the proper functioning of other foreign critical infrastructure depended on by the U.S. military and other U.S. interests overseas.[27] Even for domestic infrastructure, the exclusion policy would not protect U.S. interests in the event that the Nordic companies continue to run into financial difficulties despite positive outlooks for growth in 5G sales.[28]

Most discussion of the Huawei issue centers around "espionage;" however, the greater concern is actually availability, given that encryption and authentication technology can be used to protect confidentiality and integrity of communications. Every critical infrastructure system in the United States, including that of the USG, depends on commercial telecommunications infrastructure.[29] On the worst possible day in a conflict with a peer adversary, the United States may not be able to count on the survivability of communication satellites, and satellites do not provide sufficient data rates for the full scope of information-based warfare strategies regardless.[30] Even surviving fiber links would be subject to disruption if the communications must pass through equipment provided by vendors from hostile countries, notably Huawei and ZTE. For example, Huawei completely dominates the telecommunications infrastructure in Iraq that the USG and its military presence depend on.[31]

Current policy depends on convincing other countries to use more expensive European equipment with capabilities reportedly lagging Huawei features by a year or more.[32] U.S. policy also potentially has the effect of asking other countries to rip out existing investments in Huawei equipment prior to installing new 5G equipment, which in the case of Europe would cost more than $60 billion, according to some estimates,[33] although others suggest it would cost much less.[34] Within the United States, small rural carriers would face existential financial hardships transitioning away from Huawei.[35] This policy impact could be mitigated in part with equipment that will be available by the end of 2019 to bridge the gap between old Huawei and new western equipment.[36] To counter future transition problems, telecommunications service providers, in part through the Open Radio Access (O RAN) Alliance, are promoting the global use of interoperable standards that would allow the service providers to avoid vendor lock-in for future generations.[37]

Some countries are seeking mitigation of the threat by limiting Huawei to the "edge" of their networks and excluding Huawei from the "core;" however, telecommunications companies and U.S. Government officials have noted that, with 5G, the distinction between the edge and the core largely disappears, suggesting this approach would not satisfy U.S. security concerns.[38] The British experience with inspections of Huawei equipment highlights the challenge of guaranteeing security through inspection as another means of mitigation.[39] A nation might seek to adopt a "zero trust" model for 5G; however, industry experience in developing "trusted computing" suggests that hardware as the "root of trust" has a degree of privilege that cannot be controlled against an untrusted supplier.[40] Meanwhile, Huawei is seeking to improve its code review process to mitigate concerns raised by the British reports.[41]

Some argue that U.S. policy should solve the global problem by "killing" Huawei through the cut-off from western supply chains; however, this view ignores the likelihood that Beijing would step in to assist its national champion even more so than it has already.[42] China to date has always fallen short of the information technology state of the art and thus succumbed to the market imperative to use better western components; however, bifurcation of the global market would alter this dynamic decisively.[43] The founder and chief executive of Huawei, Ren Zhengfei, prior to the G20 summit in June 2019 said;

> *The U.S. is helping us in a great way by giving us these difficulties. If we aren't allowed to use U.S. components, we are very confident in our ability to use components made in China and other countries.*[44]

In response to U.S. policy and concern for their Chinese markets, Ericsson and Nokia reportedly are planning how they might need to bifurcate organizations and supply chains to remain in both western and Chinese markets, with potentially significant costs on top of already weak financial positions.[45]

According to Triolo and Allison of the Eurasia Group, in their paper on "The Geopolitics of 5G";

> *The United States and China also are competing to develop innovative technology applications that will run on top of deployed 5G networks. The United States has an advantage in terms of innovation capacity, but China will benefit from its head start building out its domestic 5G ecosystem and as Chinese companies then compete for market share abroad.*[46]

Triolo and Allison note that, "The push for a China-free 5G alternative is likely to delay 5G deployment where backup suppliers are forced to invest in new manufacturing capacity and human capital, further cementing China's first-mover advantage." They also note that;

> *A bifurcated 5G ecosystem would increase the risk that the global technology ecosystem would give way to two separate, politically divided technology spheres of influence. Such a split could result in some interoperability issues or lower economies of scale and higher transaction costs.*[47]

Potential Damage to the U.S. Semiconductor Industry

Meanwhile, the semiconductor industry and other high-technology industries in the United States have expressed concern about the collateral effects of the Huawei policy resulting from market "uncertainty" and the potential loss of Chinese markets, which in some cases account for a significant fraction of their revenue (for example, Qualcomm, Micron Technology, Qorvo, Broadcom, and Texas Instruments each earn more than 40 percent of their revenues from China; Intel and Nvidia get

more than 20 percent from China). Huawei depends particularly on U.S. optical and analog components from companies such as NeoPhotonics (49 percent of revenue from Huawei alone), Lumentum (18 percent), Inphi (14 percent), Qorvo (13 percent), II-VI (9 percent), and Finisar (8 percent).

Because U.S. economic policies have so strongly favored globalization, key capabilities in the high-technology sector during the past 30 years have moved overseas to a significant degree. At first this primarily involved assembly of electronic components; however, the most complex manufacturing—including for advanced printed circuit boards and semiconductors and their associated supply chains—increasingly are centered outside the United States. U.S. industry has focused on maintaining ownership of intellectual property through the design process but often depends on companies such as the Taiwan Semiconductor Manufacturing Company (TSMC) to make products.

How Did We Get to This Point?

The lack of a U.S. industrial base for integrated telecommunications equipment manufacturing that could compete with Huawei and the European firms for the global deployment of 5G systems is the direct result of a "perfect storm" of regulatory, technology, and economic shifts at the end of the 1990s. As detailed in the extensive study published in 2011 by Lazonick and March, the primary U.S. company, Lucent Technologies, ultimately failed because it made short-term financial decisions without a long-term vision for technology and global market development.[48] In particular:

- The USG breakup of the Bell System in 1984 led by 1996 to the spinoff of Western Electric manufacturing and the world renown Bell Laboratories. The new company, Lucent, was intended to serve as a neutral provider to all of the emerging U.S. service providers. Canada's Nortel had spun off from the Bell System in 1949 as a result of an earlier anti-trust suit.[49]
- Telecommunications markets benefited from the boom times of the late 1990s and early 2000s but were then crushed in the wake of a general downturn in western economies in 2001–02.
- Lucent had an incumbent advantage with legacy technologies but failed to make the pivot to internet services and applications, in part because it sought to develop its own protocols rather than use the broadly accepted Internet Protocol.
- Lucent with the help of Bell Labs, along with Canada's Nortel, made great progress in optical network technology; however, the technology was deployed far faster than anyone was prepared to use it, leading to a collapse in demand after 2000 for Lucent, Nortel, and the submarine cable business. Lucent spun off its optical cable division to Furukawa Electric in 2001. Global demand for optical networks did not recover for more than a decade.[50]
- Lucent contributed to the early expansion of mobile networks with arguably superior technology for 3G networks, such as CDMA, but failed to capture markets in Europe and Asia that used other technology such as GSM.
- Lucent in 2000 spun off its profitable microelectronics division after forcing the division to compete for Lucent business with third-party providers.
- Lucent in 2000 also spun off its "slower growing" enterprise network division, leaving the company without an ability to compete when this market segment grew faster than the general telecommunications market after the 2001–02 economic downturn.

This toxic mix led to consolidation of the integrated equipment manufacturing firms in the West

The Chinese company Huawei is establishing a dominant position in the global 5G marketplace despite concerns over security and its ties to the Chinese government. (Furicpic.pw)

even as Huawei and ZTE emerged in global markets after the worst of the downturn, building on top of rapidly modernizing and expanding infrastructure in China.[51] The UK's Marconi went through a complicated series of mergers and divestments, with the telecommunications group eventually ending up in 2005 as part of Sweden's Ericsson.[52] Ericsson in 2010 absorbed what was left of Nortel after that company collapsed into bankruptcy in 2009.[53] Finland's Nokia absorbed Motorola Solutions in 2011, and then the communications group of Germany's Siemens in 2013. Meanwhile, in 2006 France's Alcatel absorbed Lucent; however, even this new firm could not thrive and was absorbed by Nokia in 2016.[54] The only other major player to arise during this period has been South Korea's Samsung, which so far has little overall market share in telecommunications equipment but seeks to build on its mobile phone and semiconductor reputations and South Korea's investment in broadband networks.[55]

Government's Longstanding Role in Promoting Critical Infrastructure

History provides a guide for how the government could help reset the playing field with the goal of creating stronger competition against China's heavily supported national telecommunications champion. Consensus on the government's role in infrastructure development did not emerge immediately and will remain a matter of discussion in terms of when such interventions are appropriate. Discussions in the early days of the nation primarily centered on toll roads and canals that were deemed vital to commerce and military mobility for the growing nation. Competition for commercial traffic led to fights among the States until the 1824 Supreme Court decision in *Gibbons v. Ogden* ruled that the commerce clause of the U.S. Constitution granted power to regulate interstate commerce to the U.S. Congress, overriding any decisions by the States.[56] From that point forward, the U.S. Government acted more decisively.

- The U.S. Army Corps of Engineers took on a direct role in the planning, building, and management of national waterways once the U.S. Congress passed the General Survey Act of 1824.[57]
- The USG provided companies with financing and land rights for the building of the Transcontinental Railroad during the 1860s (the companies eventually paid off the loans).[58]
- During the Depression of the 1930s, the Roosevelt Administration led the effort to build dams and the national power grid to accelerate the spread of electric power.[59] [60]

The government has been involved in projects that created new infrastructure and involved long periods of investment, including for communications.

- In 1956, the Eisenhower Administration worked with the U.S. Congress to begin building the nation's Interstate Highway system of almost 50,000 miles, largely funded by the U.S. Government.[61]
- Starting in the late 1960s, the USG-funded research and development for packet-switched networks that by 1995 evolved into the commercial internet.[62] USG interest initially was to create communications that would be resilient in the event of wartime destruction of key telecommunication nodes; however, the interest pivoted to the creation of new commercial services that had been piloted inside government-funded networks.

In other cases, the government sought to create private sector capabilities that required a large investment boost to get started.

- During the 1960s, the USG under President Kennedy funded a large-scale expansion of the nation's space industry through the Apollo program.[63] In 2019 dollars, NASA spent more than $250 billion between 1960 and 1973 to put a man on the moon—creating a major impetus for communications, electronics, and computer development.[64] At its peak, the NASA budget represented more than 4 percent of the federal budget.[65]
- The international satellite communications company IntelSat, with a constellation of about 50 geostationary satellites, in the early 1960s was created by a multinational government consortium and then fully privatized by 2001.[66] InMarSat, with about a dozen geostationary satellites, has had a similar history, beginning in the late 1970s as an intergovernmental organization and transitioning to privatized operations in 1998.[67]

The government has used a combination of loans, investment, subsidies, taxes, fees, and procurement to save U.S. industry from imminent

collapse, to stimulate innovation, or to stimulate the economy as a whole.

- Since 1958 the Defense Advanced Research Projects Agency (DARPA) has funded the development of emerging technologies for military applications, most famously the networking technology that underlies the internet.[68] In the late 1980s DARPA provided matching funds for SEMATECH, an industry consortium that managed grants for semiconductor manufacturing research.[69]
- The U.S. Congress in early 1980 granted Chrysler $1.5 billion in loan guarantees to help the number three automaker recover from bankruptcy.[70] Chrysler paid off the loans in 1982.[71]
- The Department of Defense (DOD) in 2000 used procurement funds to help the Iridium satellite phone business stay afloat and remained a major customer as the infrastructure went through bankruptcy, sale, and then regeneration, because the constellation provided a unique global communications capability.[72]
- DOD in 2005 used $50 million of Title III Defense Production Act funds to restore manufacturing capabilities of high-purity Beryllium metal that had been mothballed five years earlier because of declining demand and liability for health hazards to workers.[73]
- The USG exercised a major role in preserving industry and infrastructure during times of economic difficulties, most dramatically in the wake of the 2008 financial crisis, when the U.S. Treasury and the Federal Reserve intervened on an unprecedented scale to save financial institutions and automakers on the brink of collapse resulting from bad loans. The U.S. Congress authorized the spending of up to $750 billion under the Troubled Assets Recovery Program (TARP), primarily through loans and stock purchases. Assistance to the insurance company AIG alone amounted to $182 billion. The government at one point owned 92 percent of AIG stock but over time sold all of the stock, resulting in a net gain of about $22 billion for taxpayers.[74]
- The 2009 *American Recovery and Reinvestment Act* made extensive use of tax incentives for individuals and companies, but also set aside procurement funds, all intended as a short-term economic stimulus.[75] Of almost $800 billion, only about $100 billion was specified for infrastructure, and less than a third of that went to building infrastructure (including about $7 billion for broadband internet)—illustrating the challenges for the USG to influence infrastructure either quickly or without a specified objective.[76]

The rise of the defense industrial base after World War II, which helped create "Silicon Valley," is the best example of a long-term government investment for national security purposes.[77] This capacity was nurtured throughout the Cold War with massive, long-term investments through Defense Department procurements in combination with USG capabilities and facilities. By the year 2000, however, Defense Department policies sought to control costs through commercial-off-the-shelf products and an international supply chain.[78] Policy guidance continues to be "buy, not make."[79]

Options for the Nation

Given the shortfalls of a "just say no" policy, the United States will need to compete in the telecommunications equipment integration sector, both in terms of products and trade strategy. The U.S. Government typically seeks to use procurement for federal networks and research and development investment as the primary levers for influencing high technology. U.S. industry already leads in

component and subsystem technologies (notably in optics); however, that advantage has not overcome the boom and bust cycles of the equipment integration market. Thus, a new element will be required that will involve some combination of direct investment, subsidies, loans, and tax incentives as has been done for other industries, either for national security purposes or to preserve national economic or industrial capabilities. In addition, the USG could include preferred telecommunications equipment manufacturers (no matter where they are from) in U.S. trade, defense, and foreign policy packages that the United States seeks to implement with other nations that are upgrading their telecommunications infrastructure.

Similar ideas have been raised before, including by this author and by James Lewis of the Center for Strategic and International Studies.[80] Lewis cited three options: build networks from insecure components, build a national champion, or subsidize European producers. According to Lewis, the Obama Administration considered funding a national champion using the *Defense Production Act*, "but it could at most allocate 1 percent of what China spent. The discussion of how to respond to the telecom problem made it as far as a Deputies Committee meeting, but none of the major information technology companies wanted to reenter this field. Though a few medium-size companies could have been candidates for investment, the administration ultimately decided to rely on Google and Silicon Valley to innovate our way out of the problem without the need for the government to spend anything."

The U.S. Defense Science Board's June 2019 report on "Defense Applications of 5G Network Technology" notes that "the lack of a U.S. integrator and Radio Access Network vendor industrial base" creates challenges. The report recommends that the Department of Defense "should provide seed funding for western industrial base alternatives of key system components, e.g., Radio Access Networks."[81]

The scale of investment required—as can be seen from the size of the European companies—would require the U.S. Congress to appropriate additional funds, even if implemented under existing authorities, such as Title III of the *Defense Production Act* (annual appropriations typically range only in the 10s to 100s of millions of dollars).[82] Ericsson and Nokia each employ about 100,000 or more workers (although not just for telecommunications integrated equipment manufacturing), and each as of 2018 had net equities in the range of $10-20 billion and net assets in the range of $25–45 billion.[83] Nokia spent $16.6 billion acquiring Alcatel–Lucent in 2016.[84]

Maintaining leadership requires huge research investments. Huawei is participating comprehensively in the international standards process and makes large investments in research and development, now increasing to $15–20 billion per year from levels of $13–15 billion in 2017–18.[85] European firms lag significantly. Nokia has increased investment in research and development to about 20 percent of its revenue or roughly $5 billion per year after a significant decline during 2013–15.[86] In addition, the European Investment Bank in August 2018 provided a $583 million five-year loan to Nokia in 2018, and Canada in January 2019 provided Nokia with a $40 million research grant.[87] Ericsson in 2017 increased investments to at least 15 percent of its revenue—a bit more than $4 billion per year—despite concurrent net income losses.[88]

The major U.S. telecommunications service providers with operations in the United States and abroad would need to be included at least in the planning process for such an investment policy given that they would be the ultimate customers for most of the equipment, have expertise on the markets and systems and, most likely, would serve as the final systems integrators and operators during implementation and deployment. Indeed, the service providers could be provided incentives

to participate directly in the investment strategy; however, they are also burdened with high levels of debt from capital expenditures.[89] Other operators of critical infrastructure (financial systems, electric power, oil and gas distribution, transportation, etc.) also might benefit by participating in the planning and investments.

The following three options are not mutually exclusive.

Option 1: Champion the European and South Korean Companies

U.S. telecommunications infrastructure already depends on Ericsson and Nokia (and to a much lesser degree on Samsung[90]), each of which have a significant economic presence through their U.S. subsidiaries. As noted previously, these companies include some of the residual capabilities that once belonged to now-defunct U.S. integrated telecommunications equipment companies. The USG, perhaps working primarily through the U.S. subsidiaries, might be able support these companies with stock investments, tax policies, debt guarantees, loans, and procurements, particularly to stabilize their finances and to boost their research and development investments that lag significantly behind those of Huawei. Both companies have undergone significant adjustments in management and business portfolios to stabilize their financial situation while investing for future growth. Both companies expect global demand to grow as most countries seek to take advantage of the benefits of 5G. In the unlikely event that the two Nordic companies merged to gain economies of scale relative to Huawei (despite potential EU, Chinese, and U.S. anti-monopoly concerns and challenges merging product lines), the USG could support the new merged entity in the same way.

> *As a sign of the Samsung's commitment to diversifying its product line, press reports in July 2019 indicated that Samsung plans to invest more than $100 billion over the next 10 years to gain prominence in global chip processors.*[91] *Samsung, however, in November 2019 announced the closure of its US-based research lab for mobile phone chips after failing to win market share from Qualcomm from external customers.*[92]

Option 2: U.S. Entities Acquire Either or Both European Companies

If the United States needs to have a home-based champion for 5G and beyond, the fastest approach might involve working with the private sector to acquire a controlling interest in parts of one of the existing European companies, possibly using authorities under the Defense Production Act Title III or else with a separate Congressional authorization. Nokia Networks would be the primary division of interest from Nokia along with Bell Labs, and Business Area Networks would be the key division within Ericsson.[93] Samsung's 5G segment may not be a good target for acquisition because it has much less market share and is part of a growth strategy for the otherwise very large vertically integrated South Korean conglomerate.[94]

- The USG could use past models of loan guarantees, tax incentives, and direct investment. Either of these companies would benefit from significant U.S.-based investment and more innovative and agile management to help them stabilize their finances and close the gap in research and development that these companies have with Huawei.
- Both companies have significant presence in the United States and recently have sought to expand their U.S. research and production. For example, Ericsson plans to open a fully automated factory for advanced antenna systems in the United States by 2020 and previously set up a design center in Texas for

5G-related application specific integrated circuits (ASICs).[95] Nokia is expanding its operations in Texas, and operates the original Bell Labs facilities in New Jersey.[96]

- These companies, however, are major contributors to the economies of their home countries, suggesting a major acquisition might be resisted by those governments and the European Union.
- For example, Nokia owns Alcatel Submarine (undersea cables) that competes with the U.S. company now known as Subcom, as well as the optical networking capabilities of Alcatel–Lucent, and is likely to be seen by the Europeans (particularly Paris) as an asset that needs to remain European.[97] Meanwhile, Ericsson is not a major player in optical networks and depends more on microwave for backhaul communications.[98]
- In addition, these companies have facets unrelated to integrated telecommunications equipment manufacturing that are, in part, artifacts of prior mergers and acquisitions. Culling out the equipment manufacturing alone, however, might leave behind unsustainable business organizations. Also, as Lucent experienced, the equipment manufacturing by itself may not be sustainable through demand cycles.[99] These companies also have existing business arrangements and obligations, in some cases with China, that may create complications for U.S. trade policy.[100]

Option 3: Create a U.S.-Based Consortium

The USG could seek to create business conditions through a combination of procurement, investment, and financing to bring together the robust, diverse capabilities of existing U.S. private sector capabilities and patent rights that foreign integrated telecommunications equipment manufacturers already depend on under an integrated corporate management. Private equity could supplement USG funds, leading over time to an eventual reduction in the share of government investment while maintaining U.S. financial guarantees and trade support in the background.

Over time, this "consortium" could be led by a "prime" company comparable to the big integration companies that dominate U.S. defense contracting. Such an entity could add or even subtract "sub-prime" capabilities as needed in accordance with changes in technology, fluctuating demand, and maturation of national infrastructures. Again, the USG could use combinations of past strategies to drive the formation of this consortium, with the ultimate goal of leaving the private sector in control.

- Rather than be treated as direct competitors, Nokia and Ericsson could contribute subsystems (particularly for radio access networks)—as might other companies from trusted international partners, notably the Five Eyes, Germany, France, Japan, and South Korea.
- Such an approach could in effect create a single, trusted U.S.-based, international consortium with the financial backing of the USG for use by U.S. allies and any nation that would trust such an alliance more than Chinese providers.
- Success would depend on a competitive pricing strategy in combination with U.S. and allied incentives to participate. Such a consortium also would benefit from strong relationships with the U.S. and allied defense departments and ministries.

A Bottom Line Comparison of Options

Each option involves positive and negative tradeoffs. All of them face potential resistance from overseas, including the Nordic countries, the EU (especially

France), and possibly China. The resistance could be regulatory or through the WTO.

- **Support to an existing foreign firm** would involve the least commitment from either the USG or private sector; however, this option offers the least influence or certainty of a useful result.
- **Buying one of the two Nordic firms** would be easier than creating a new corporate entity and the fastest way back into the telecommunications equipment integration business but would require greater investment than simply supporting a firm with its current ownership. The United States would not have as much leverage on the outcome as would occur with the purchase of both firms.
- **Creating a new consortium** would be the hardest to implement in terms of creating product lines, gaining market share, and licensing patents but would offer the greatest control of the outcome and thus the best opportunity to invest for longer-term technologies. As a result, this option potentially would require the greatest investment but also has the potential for the greatest return in terms of U.S. jobs and stimulating the U.S. high-technology sector.

Economic success of the strategy would depend on international trust of the equipment provider. In some parts of the world, U.S. ownership would provide comfort; however, in other parts of the world even some friendly countries might prefer "neutral" European products, a potentially useful outcome if the U.S. policy goals include not undermining a viable European competitor. In any case, western entities will need to persuade potential customers that the reliability and quality of products combined with transparent security policies is an attractive feature in comparison to what is offered by Chinese alternatives.

The final implementation of 5G will represent more than an upgrade to 4G technology components; the new systems over many years will evolve to a fundamentally different architecture and drive massive changes in the infrastructures and businesses that will benefit from 5G.[101] With this longer perspective in mind, the best U.S. strategy might involve a combination of the options. In the near-term, the United States needs to "get in the game," perhaps through options 1 or 2, to avoid surrendering future incumbent advantages to China and to gain experience in working with the new systems. For the long run, however, the United States as a second step might need to focus on the broader U.S. high-technology industry with Option 3 to drive innovation and to be in the best position for future generations.

The deployment of 5G technology across all of the infrastructure will take at least 10 years; however, discussion of 6G technology has already begun. In November 2018 a Chinese official claimed that the Ministry of Information and Industry Technology had already begun work on 6G with a view toward initial commercial deployments as early as 2030.[102] Finland's Oulu University's 6Genesis Project seeks to develop communication networks with bandwidths over 1 terabit per second with a grant of more than $250 million.[103] As the Finnish researchers note, 6G will build on 5G infrastructure and applications, and thus any investment in 6G will need to build on a prior investment in 5G.

Find a USG Champion

Justification for the amount of resources needed to reboot the nation's supply chain for integrated telecommunications systems would need to be framed in terms of ongoing U.S. strategies for resilient global command and control systems for national security and for maintaining control of critical infrastructure functions under the most stressful circumstances of a war with a peer adversary, such as Russia or China. This level of demand is a unique national-level governmental requirement and thus must be met at least in part by the USG. The measure of success would be determined by whether U.S. defense and

critical infrastructure planners could demonstrate greater resilience against the full spectrum of threats. The U.S. military already is seeking to improve the resilience of critical systems, including for nuclear command, control and communications (NC3).[104]

The biggest player within the USG, and the most likely center point for a successful effort, would have to be Department of Defense. This is the only department with the global reach and mission requirements, technical depth, procurement and large-scale integration experience, budgetary capacity, and existing authorities to handle such a large project. The Office of the Secretary of Defense would need to work with the Joint Chiefs of Staff to incorporate military strategic requirements and with the Department of Homeland Security and other government agencies that work with private sector critical infrastructure.

Conclusion: Resiliency Strategy Must Determine the Way Forward

As noted by West Point authors Borghard and Lonergan, the United States needs to examine its policies toward the next generation of telecommunications in the context of strategic requirements for resilient global command and control of U.S. military forces and other U.S. interests, to include how the U.S. military depends on commercial communications.[105] This discussion must consider the worst possible day, not the routine day. The challenge is primarily one of availability on that worst day, not espionage. These requirements abroad and for critical infrastructure at home are uniquely the purview of government, and thus the government must step up and make the strategic investment in what is essentially the central nervous system of the nation. An effort of this magnitude will require a unified approach across the Executive Branch and broad bipartisan support from the U.S. Congress.

Trade policy alone, particularly one given to broader compromise, will not allow the United States to define how other nations choose to implement infrastructure that U.S. national security communications may need to pass through. The United States needs a unified vision of how to compete in terms of technology and close deals for U.S. advantage. As with the defense industrial base, the USG in the long run should seek to have the private sector operate any new manufacturing capability and thus would need to work in partnership with the industries that best understand the technology and customer needs. The USG would need to stand behind industry efforts to gain deals with other nations—just as it has for other vital industries with national security implications, notably aviation.

The USG, as it has with most national security efforts abroad, would need assistance from traditional national security allies and countries located at what already are or should be key communications junctures.[106] For example, new pathways might be needed that are less vulnerable to disruption as compared to the ones now passing where they are vulnerable to adversary disruption, through areas of dense commercial activities, or in regions of longstanding conflicts.[107] As has been done for some military systems, the United States would need to work with trusted nations that can provide useful technology and manufacturing capacity, in part to gain their support for a new player in the integrated telecommunications market place.

It will not be enough for the private sector with government support just to create a company to manufacture and integrate telecommunications systems. The USG, in partnership with the private sector, will need to consider how it will remain competitive over the long term.

- This may require financial support to help industry get through demand lulls, including if demand lags expectations, as occurred from 2000 to 2010, because of slower than expected implementation of applications elsewhere in U.S. infrastructure and businesses.

- In addition, a long-term strategy would require reinvigoration of investment in the hardware elements all across the U.S. high-technology sector that have either moved to Asia or been too long dependent on investments made years ago.[108] A telecommunications equipment integrator based in the United States would provide an anchor for investment in all of the component technologies and their associated supply chains, including future generations of semiconductors. The success of innovation in the U.S. high technology sector will depend on preserving homeland-based manufacturing and supply chain ecosystems.

Key challenges going forward include mobilizing the USG to act and then drawing in the right elements of the private sector as investors or participants in product development. Then the real work would begin with developing a product line that can compete in terms of the best combination of technology, pricing, and financing. Additional incentives from U.S. and allied governments might be needed to overcome incumbent advantages or to walk back some past infrastructure decisions in key, strategic locations.[109]

This will be a "long march" (as China's President Xi would say). But better to start now than repeat this conversation in 10 years. PRISM

Notes

[1] Wikipedia "Anti-satellite weapon," available at <https://en.wikipedia.org/wiki/Anti-satellite_weapon>; Garrett Hinck, "Evaluating the RU.S.sian Threat to Undersea Cables," Lawfare, March 5, 2018, available at <https://www.lawfareblog.com/evaluating-rU.S.sian-threat-undersea-cables>.

[2] Emma Vickers, "The 70-Year Spy Alliance the U.S. Says It May Cut Off," Bloomberg Businessweek, June 30, 2019, available at <https://www.bloomberg.com/news/articles/2019-06-30/the-70-year-spy-alliance-the-u-s-says-it-may-cut-off-quicktake>.

[3] Thomas Oliphant, "Inside Kennedy's Quest to put America on the Moon," review of *American Moonshot: John F. Kennedy and the Great Space Race*, by Douglas Brinkley, *The Washington Post*, April 4, 2019, available at <https://www.washingtonpost.com/outlook/inside-kennedys-quest-to-put-america-on-the-moon/2019/04/04/6bd26cac-499c-11e9-93d0-64dbcf38ba41_story.html>.

[4] National Research Council, "Renewing U.S. Telecommunications Research, Chapter 1:The Importance of Telecommunications and Telecommunications Research," The National Academies Press, available at <https://www.nap.edu/read/11711/chapter/3#10>.

[5] Peter Lewis, "U.S. Begins Privatizing Internet's Operations," *The New York Times*, October 24, 1994, available at <https://www.nytimes.com/1994/10/24/bU.S.iness/U.S.-begins-privatizing-internet-s-operations.html>.

[6] Sean Buckley, "Telco Capex: AT&T, Verizon Remain Kings, While CenturyLink, Frontier and Windstream Adjust Integration, Cost-containment Plans," April 11, 2018, available at <https://www.fiercetelecom.com/telecom/telco-capex-at-t-verizon-remain-kings-while-centurylink-frontier-and-windstream-adjU.S.t>;Antonio Cosma and Ugur Bitiren, "Increasing Focus on Working Caapital in the Telecoms Industry," Connectivity Busiiness, July 2018, available at <https://www.ca-cib.com/sites/default/files/2018-07/Connectivity-BU.S.iness-Telecoms-IndU.S.try.pdf>.

[7] Quexor Group, "10 years of Consolidation in Wireless: The Rise of Verizon, AT&T, T-Mobile and Sprint," *Fierce Wireless*, 2015, available at <http://assets.fiercemarkets.net/public/mdano/amis/wireless-consolidation1.jpg>; Harry McCracken, "A Brief History of the Rise and Fall of Telephone Competition in the U.S., 1982-2011, Technologizer, March 20, 2011, available at <https://www.technologizer.com/2011/03/20/att-buys-t-mobile/>; Roger Cheng and Marguerite Reardon, "The T-Mobile-Sprint Deal May Close Soon: Here's What you Need to Nnow," C-Net, July 5, 2019, available at <https://www.cnet.com/news/t-mobile-sprint-deal-may-close-soon-heres-what-you-need-to-know/>.

[8] William Lazonick and Edward March, "The Rise and Demise of Lucent Technologies," 2011, available at <http://thebhc.org/sites/default/files/lazonickandmarch.pdf>; Brian Fung, "How China's Huawei Took the Lead over U.S. Companies in 5G Technology, *The Washington Post*, April 10, 2019, available at <https://www.washingtonpost.com/technology/2019/04/10/U.S.-spat-with-huawei-explained/?utm_term=.079c8eb7d3c8>; Stratfor, "The U.S., China and Others Race to Develop 5G Mobile Networks," April 3, 2018, available at <https://worldview.stratfor.com/

article/U.S.-china-and-others-race-develop-5g-mobile-networks>.

[9] Martha DeGrasse, "Ericsson Widens Lead over Nokia in U.S. Equipment Markets: Analysts," Fierce Wireless, May 11, 2018, available at <https://www.fiercewireless.com/5g/u-s-5g-helping-ericsson-gain-ground-huawei>; FCC WC Docket No. 18–89, "Protecting Against National Security Threats To the Communications Supply Chain Through FCC Programs," December 7, 2018, available at <https://ecfsapi.fcc.gov/file/12080817518045/FY%202019%20NDAA%20Reply%20Comments%20-%20FINAL.pdf>.

[10] Moody's Investors Service, "Rating Action: Moody's changes the outlook on Nokia's ratings to negative," February 8, 2019, available at <https://www.moodys.com/research/Moodys-changes-the-outlook-on-Nokias-ratings-to-negative--PR_394891>; Moody's Investors Service, "Rating Action: Moody's changes the outlook on Ericsson's ratings to negative," July 18, 2018, available at <https://www.ericsson.com/assets/local/investors/documents/bondholder-information/rating/moodys/moodys_180718.pdf>; Parmy Olson, "With Huawei on Defensive, Ericsson and Nokia Fight Each Other for Edge," *The Wall Street Journal*, May 29,2019, available at <https://www.wsj.com/articles/with-huawei-on-defensive-ericsson-and-nokia-fight-each-other-for-edge-11559122200?ns=prod/accounts-wsj>.

[11] Richard Milne, "Nokia shares plunge on 5G outlook in US and China," *Financial Times*, 24 October 2019, available at https://www.ft.com/content/1fff9178-f62c-11e9-9ef3-eca8fc8f2d65

[12] Stefan Pongratz, "Key Takeaways—Worldwide Telecom Equipment Market 2018," Dell'Oro Group, March 4, 2019, available at <https://www.delloro.com/telecom-equipment-market-2018-2/>.

[13] Eric Auchard and Sijia Jiang, "China's Huawei set to lead global charge to 5G networks," *Reuters*, February 23, 2018, available at <https://www.reuters.com/article/U.S.-telecoms-5g-china/chinas-huawei-set-to-lead-global-charge-to-5g-networks-idU.S.KCN1G70MV>.

[14] Stu Woo, "Huawei Rivals Nokia and Ericsson Struggle to Capitalize on U.S. Scrutiny," *The Wall Street Journal*, December 31, 2018, available at <https://www.wsj.com/articles/huawei-rivals-nokia-and-ericsson-struggle-to-capitalize-on-u-s-scrutiny-11546252247>.

[15] Ellen Nakashima, "U.S. Pushes Hard for a Ban on Huawei in Europe, but the Firm's 5G prices are nearly Irresistible," *The Washington Post*, May 28, 2019, available at <https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-U.S.-is-pU.S.hing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html>.

[16] Li Tao, "Nearly 60 percent of Huawei's 50 5G contracts are from Europe," *South China Morning Post*, July 19, 2019, available at <https://www.scmp.com/tech/big-tech/article/3019248/nearly-60-huaweis-50-5g-contracts-are-europe>.

[17] Jeff Pao, "Chinese Telecoms Unveil their 5G Strategies," Asia Times, June 28, 2019, available at <https://www.asiatimes.com/2019/06/article/chinese-telecoms-unveil-their-5g-strategies/>; Frank Chen, "A look at Shenzhen and Huawei's 'Smart City' Project," *Asia Times*, July 11, 2019, available at <https://www.asiatimes.com/2019/07/article/a-look-at-shenzhen-and-huaweis-smart-city-project/>; Darlie Yiu, "Shanghai to be 'Intelligent Manufacturing' Hub," *Asia Times*, June 25, 2019, available at <https://www.asiatimes.com/2019/06/article/shanghai-to-be-intelligent-manufacturing-hub/>; Jeff Pao, "China Unicom to Build 5G Networks on Belt and Road," *Asia Times*, June 25, 2019, available at <https://www.asiatimes.com/2019/06/article/china-unicom-to-build-5g-networks-on-belt-and-road/>.

[18] Yuan Yang, James Kynge, Sue-Lin Wong, and Nian Liu, "Huawei Founder Predicts Internet of Things is Next U.S. Battle," *Financial Times*, July 3, 2019, available at <https://www.ft.com/content/716181ce-9bd8-11e9-9c06-a4640c9feebb>.

[19] Raymond Zhong, "'Prospective Threat' of Chinese Spying JU.S.tifies Huawei Ban, U.S. Says," *The New York Times*, July 5, 2019, available at <https://www.nytimes.com/2019/07/05/technology/huawei-lawsuit-U.S.-government.html>; Cassell Bryan-Low et al., "Hobbling Huawei: Inside the U.S. War on China's Tech Giant," *Reuters*, May 21, 2019, available at <https://www.reuters.com/investigates/special-report/huawei-U.S.a-campaign/>.

[20] Jim Wolf, "U.S. Lawmakers Seek to Block China Huawei, ZTE U.S. Inroads," Reuters, October 7, 2012, available at <https://www.reuters.com/article/U.S.-U.S.a-china-huawei-zte/u-s-lawmakers-seek-to-block-china-huawei-zte-u-s-inroads-idU.S.BRE8960NH20121008>.

[21] British Cabinet Office, "Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2018," July 19, 2018, available at <https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018>; Davey Winder, "GCHQ Director Says 'Shoddy' Huawei Security Engineering Belongs in the Year 2000," *Forbes*, April 8, 2019, available at <https://www.forbes.com/sites/daveywinder/2019/04/08/gchq-director-says-shoddy-huawei-security-engineering-belongs-in-the-year-2000/#4f0d1deeafe6>; Finite State, "Supply Chain Assessment: Huawei Technologies Co.,

Ltd.," June 2019, available at <https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf>.

[22] Salem Solomon, "After Allegations of Spying, African Union Renews Huawei Alliance," VOA, June 6, 2019, available at <https://www.voanews.com/africa/after-allegations-spying-african-union-renews-huawei-alliance>; John Aglionby, Emily Feng, and Yuan Yang, "African Union Accuses China of hacking headquarter," *Financial Times*, January 29, 2018, available at <https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5>.

[23] White House, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019, available at <https://www.whitehoU.S.e.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>; Bureau of Industry and Security, Commerce, "Addition of Entities to the Entity List," 84 Fed. Reg. 22961, May 21, 2019, available at <https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list>.

[24] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-874, Section 889, 115th Cong. (2018), available at <https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf>.

[25] David Phelan, "Trump Surprises G20 With Huawei Concession: U.S. Companies Can Sell To Huawei," *Forbes*, June 29, 2019, available at <https://www.forbes.com/sites/davidphelan/2019/06/29/trump-surprises-g20-with-huawei-concession-u-s-companies-can-sell-to-huawei/#7f520a11e212>; Kiran Stacey, "U.S. Announces Significant Relaxation of Huawei Ban," *Financial Times*, July 9, 2019, available at <https://www.ft.com/content/301d6d9c-a2a7-11e9-974c-ad1c6ab5efd1>.

[26] United States 5G Leadership Act of 2019, S. 1625 (introduced), 116th Cong. (2019), available at <https://www.govtrack.U.S./congress/bills/116/s1625/text>; Secure 5G and Beyond Act of 2019, S.893, 116th Cong. (2019), available at <https://www.govtrack.U.S./congress/bills/116/s893/text>.

[27] David Vine, "U.S. Military Bases Abroad, 2015," Base Nation, 2015, available at <https://www.basenation.U.S./maps.html>.

[28] Markets Insider, "Ericsson (Telefon AB L.M. Ericsson) (B) Outperform," June 18, 2019, available at <https://markets.bU.S.inessinsider.com/analysts-opinions/ericsson-telefon-ab-l-m-ericsson-b-outperform-675287<; Market Beat, "NYSE:NOK-Nokia Oyj Stock Price, News, & Analysis," viewed July 17, 2019, available at <https://www.marketbeat.com/stocks/NYSE/NOK/>; Seeking Alpha, "Ericsson, Nokia to benefit from 5G cycle BofAML," May 22, 2019, available at <https://seekingalpha.com/news/3466082-ericsson-nokia-benefit-5g-cycle-bofaml>.

[29] "Telecommunications: Addressing Potential Security Risks of Foreign-Manufactured Equipment" GAO-13-652T (Statement of Mark L. Goldstein, Director Physical Infrastructure Issues Government Accountability Office, May 21, 2013), available at <https://www.gao.gov/assets/660/654763.pdf>; "Information Technology: Major Federal Networks That Support Homeland Security Functions," GAO-04-35 (A GAO Report to Congressional Requesters, September 2004), available at <https://www.gao.gov/new.items/d04375.pdf>; Department of Defense, "Department of Defense Information Network (DODIN) Transport," Instruction 8010.01, September 10, 2018, available at <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf?ver=2018-09-10-082254-477>.

[30] Sandra Erwin, "Air Force Gen. Pawlikowski: Military Satellites will be Smaller, More Mobile," *Space News*, May 15, 2018, available at <https://spacenews.com/air-force-gen-pawlikowski-military-satellites-will-be-smaller-more-mobile/>; Michael Matis, "The Protection of Undersea Cables: A Global Security Threat" (master's thesis, U.S. Army War College, 2012), available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/a561426.pdf>.

[31] Shaun Waterman, "Chinese Firm 'Owns' Telephone System in Iraq," *Washington Times*, February 21, 2011, available at <https://www.washingtontimes.com/news/2011/feb/21/chinese-telecom-end-ties-U.S.-high-tech-start-/>.

[32] Stu Woo, "Huawei Rivals Nokia and Ericsson Struggle to Capitalize on U.S. Scrutiny," The Wall Street Journal, December 31, 2018, available at <https://www.wsj.com/articles/huawei-rivals-nokia-and-ericsson-struggle-to-capitalize-on-u-s-scrutiny-11546252247?ns=prod/accounts-wsj>; Newley Purnell et al. "U.S. Campaign Against Huawei Runs Aground in an Exploding Tech Market," *The Wall Street Journal*, February 21, 2019, available at <https://www.wsj.com/articles/india-a-pivotal-internet-market-isnt-buying-u-s-campaign-against-huawei-11550762080>; Niharika Mandhana, "In Global Tech Battle, a Balky U.S. Ally Chooses China," The Wall Street Journal, July 15, 2019, available at <https://www.wsj.com/articles/in-global-tech-battle-the-philippines-has-chosen-sides-not-the-u-s-11563205891>.

[33] Asia Times staff, "Banning Huawei 'Would Cost EU Operators $62m [sic]'," *Asia Times*, June 9, 2019, available at<https://www.asiatimes.com/2019/06/article/banning-huawei-would-cost-eu-operators-62m/>.

[34] Strand Consult, "The real cost to rip and replace

of Chinese equipment in telecom networks," September 2019, Copenhagen, available at http://www.strandconsult.dk/sw8402.asp; also described by Roslyn Layton, "To Rip and Replace Huawei in EU Mobile Networks Costs About $7 per Subscriber," *Forbes*, 23 September 2019, available at https://www.forbes.com/sites/roslynlayton/2019/09/23/to-rip-and-replace-huawei-in-eu-mobile-networks-costs-about-7-per-subscriber/#20093a981c8f

[35] FCC "Protecting Against National Security Threats To the Communications Supply Chain Through FCC Programs," WC Docket No. 18-89, December 7, 2018, available at <https://ecfsapi.fcc.gov/file/12080817518045/FY%202019%20NDAA%20Reply%20Comments%20-%20FINAL.pdf>.

[36] Harri Holma, "Nokia 5G Radio: Simple to Deploy on Top of Another Vendor's 4G," Nokia, March 26, 2019, available at <https://www.nokia.com/blog/nokia-5g-radio-simple-deploy-top-another-vendors-4g/>.

[37] Matt Kapko, "AT&T Aims to 'Break the Vendor and Technology Lock-In'," SDX Central, April 5, 2019, available at <https://www.sdxcentral.com/articles/news/att-aims-to-break-the-vendor-and-technology-lock-in/2019/04/>; Corinne Reichert, "Verizon: Multi-vendor Interoperability Key for 5G," ZDNet, June 27, 2017, available at <https://www.zdnet.com/article/verizon-multi-vendor-interoperability-key-for-5g/>; O-RAN Alliance, "Operator Defined Next General RAN Architecture and Interfaces," viewed July 23, 2019, available at <https://www.fiercewireless.com/wireless/o-ran-aims-to-eliminate-vendor-lock-at-radio-access-network>; Kathy Cacciatore, "The Interoperability Challenge in Telecom and NFV Environments: A Tutorial," SuperU.S.er, April 20, 2017, available at <https://superU.S.er.openstack.org/articles/interoperability-telecom-nfv-tutorial/>.

[38] Kiran Stacey, "UK's Approach to Huawei is Flawed, Warns Ericsson's U.S. Boss," *Financial Times*, June 23, 2019, available at <https://www.ft.com/content/a91825e2-8e17-11e9-a24d-b42f641eca37>;and Nakashima, May 28, 2019.

[39] British Cabinet Office, "Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2018," July 19, 2018, available at <https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018>; Davey Winder, "GCHQ Director Says 'Shoddy' Huawei Security Engineering Belongs in the Year 2000," *Forbes*, April 8, 2019, available at <https://www.forbes.com/sites/daveywinder/2019/04/08/gchq-director-says-shoddy-huawei-security-engineering-belongs-in-the-year-2000/#4f0d1deeafe6>.

[40] Palo Alto Networks, "What is a Zero Trust Architecture," viewed July 17, 2019, available at <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trU.S.t-architecture<; Trusted Computing Group, "Where Trust Begins," viewed July 17, 2019, available at <https://trU.S.tedcomputinggroup.org/wp-content/uploads/INFOGRAPHIC-TCG-PR-Works-FINAL.pdf>.

[41] Jeff Pao, "Huawei Ensures Cyber Security with a Huge Transformation," *Asia Times*, July 22, 2019, available at <https://www.asiatimes.com/2019/07/article/huawei-ensures-cyber-security-with-a-huge-transformation/?_=1981968>.

[42] Jun Mai, "Bannon Says Killing Huawei More Important than Trade Deal with China," *South China Morning Post* (reprinted by Politico), 22 May 2019, available at https://www.politico.com/story/2019/05/22/steve-bannon-huawei-trade-china-1464607; Louise Lucas et al., "Can Huawei survive U.S. blacklisting?", *Financial Times*, May 16, 2019, available at <https://www.ft.com/content/21727292-7796-11e9-bbad-7c18c0ea0201<; Fareed Zakaria, "The Blacklisting of Huawei Might be China's Sputnik Moment," *The Washington Post*, May 23, 2019, available at <https://www.washingtonpost.com/opinions/global-opinions/the-blacklisting-of-huawei-might-be-chinas-sputnik-moment/2019/05/23/9352fc66-7d99-11e9-a5b3-34f3edf1351e_story.html?hpid&utm_term=.ee87fea2f279>.

[43] Yoko Kubota and Dan Strumpf, "American Threat to Huawei's Chip Maker Shows Chinese Tech Isn't Self-Sufficient," *The Wall Street Journal*, June 2, 2019, available at<https://www.wsj.com/articles/huaweis-main-chip-maker-faces-long-term-risks-from-u-s-ban-11559467846>; Yingzhi Yang and Li Tao, "Inside Huawei's Secretive Plans to Develop an Operating System to Rival Google's Android," South China Morning Post, June 11, 2019, available at <https://www.scmp.com/tech/big-tech/article/3013813/inside-huaweis-secretive-plans-develop-operating-system-rival-googles>; Li Tao, "Huawei Keeps Market Guessing Whether New Honor Smart Displays will run on its own Hongmeng OS," *South China Morning Post*, July 16, 2019, available at <https://www.scmp.com/tech/enterprises/article/3018680/huawei-keeps-market-guessing-whether-new-honor-smart-displays-will>.

[44] James Kynge et al. "Huawei: still Fighting for Survival Despite Trump Truce," *Financial Times*, July 3, 2019, available at <https://www.ft.com/content/a6db14d8-9993-11e9-9573-ee5cbb98ed36>.

[45] Anna Isaac, "Nokia and Ericsson Plan Emergency Break-up over Trade War and Security Fears," *The Telegraph*, June 8, 2019, available at <https://www.telegraph.co.uk/bU.S.iness/2019/06/08/exclU.S.ive-nokia-andericsson-plan-emergency-break-up-trade-war/>.

[46] Paul Triolo and Kevin Allison, "The Geopolitics of 5G," Eurasia Group, November 15, 2018, available at <https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g>.

[47] Ibid.

[48] William Lazonick and Edward March, "The Rise and Demise of Lucent Technologies," 2011, available at <http://thebhc.org/sites/default/files/lazonickandmarch.pdf>.

[49] Wikipedia, "Nortel," viewed July 17, 2019, available at <https://en.wikipedia.org/wiki/Nortel>.

[50] G.P. Agrawal, "Optical Communication: Its History and Recent Progress," in *Optics in Our Time: Its History and Our Progress*, ed. M. Al-Amri et al., (Cham, Switzerland: Springer Nature, 2016), 177-199, available at <https://link.springer.com/chapter/10.1007/978-3-319-31903-2_8>.

[51] Keith Johnson and Elias Groll, "The Improbable Rise of Huawei," Foreign Policy, April 3, 2019, available at < https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/>.

[52] Wikipedia, "Marconi Communications," viewed July 17, 2019, available at <https://en.wikipedia.org/wiki/Marconi_Communications>.

[53] Wikipedia, "Nortel," viewed July 17, 2019, available at <https://en.wikipedia.org/wiki/Nortel>.

[54] Trefis Team, "Nokia's $16.6 Billion Acquisition of Alcatel-Lucent Explained," Forbes, April 16, 2015, available at <https://www.forbes.com/sites/greatspeculations/2015/04/16/nokias-16-6-billion-acquisition-of-alcatel-lucent-explained/#58334cc2605c>.

[55] Cho Mu-Hyun, "Samsung and 5G: Will this time be different?", ZDNet, February 1, 2019, available at <https://www.zdnet.com/article/samsung-and-5g-will-this-time-be-different/>; Kenichi Yamada, "Samsung Earmarks $22bn for Nurturing New Fields," *Nikkei Asian Review*, August 8, 2018, available at <https://asia.nikkei.com/Asia300/Samsung-earmarks-22bn-for-nurturing-new-fields2>.

[56] Wikipedia, "History of Turnpikes and Canals in the United States," viewed July 17, 2019, available at <https://en.wikipedia.org/wiki/History_of_turnpikes_and_canals_in_the_United_States>.

[57] Wikipedia, "United States Army Corps of Engineers," viewed July 17, 2019, available at < https://en.wikipedia.org/wiki/United_States_Army_Corps_of_Engineers>.

[58] Maury Klein, "Financing the Transcontinental Railroad," Gilder Lehrman Institute of American History, viewed July 17, 2019, available at <https://ap.gilderlehrman.org/essays/financing-transcontinental-railroad>.

[59] David Billington et. al, "The History of Large Federal Dams: Planning, Design, and Construction in the Era of Big Dams," Bureau of Reclamation/Interior, 2005, available at <https://www.U.S.br.gov/history/HistoryofLargeDams/LargeFederalDams.pdf>.

[60] Wikipedia, "Rural Electrification Act," viewed July 17, 2019, available at <https://en.wikipedia.org/wiki/Rural_Electrification_Act>.

[61] Federal Highway Administration, "History of the Interstate Highway System," June 27, 2017, available at <https://www.fhwa.dot.gov/interstate/history.cfm>; Wikipedia, "Interstate Highway System," viewed July 17, 2019, available at <https://en.wikipedia.org/wiki/Interstate_Highway_System>.

[62] Kim Ann Zimmermann and Jesse Emspak, "Internet History Timeline: ARPAnet to the World Wide Web," Live Science, June 27, 2017, available at <https://www.livescience.com/20727-internet-history.html>.

[63] Douglas Brinkley, review of American Moonshot, 2019; Greg Ip, "The Moonshot Mind-Set Once Came from the Government No Longer," *The Wall Street Journal*, July 14, 2019, available at <https://www.wsj.com/articles/the-moonshot-mind-set-once-came-from-the-government-no-longer-11563152820?mod=hp_lead_pos5>.

[64] The Planetary Society, "How much did the Apollo program cost?", viewed July 17, 2019, available at <http://www.planetary.org/get-involved/be-a-space-advocate/become-an-expert/cost-of-apollo-program.html >.

[65] Henry Mance and Yuichiro Kanematsu, "Why NASA's next Moon Mission Can't be an Apollo Retread," *Financial Times*, July 5, 2019, available at <https://www.ft.com/content/5adc069a-9d27-11e9-b8ce-8b459ed04726>.

[66] Wikipedia, "Intelsat," viewed July 17, 2019, available at <https://en.wikipedia.org/wiki/Intelsat>.

[67] Wikipedia, "Inmarsat," viewed July 17, 2019, available at<https://en.wikipedia.org/wiki/Inmarsat>.

[68] Defense Advanced Research Projects Agency, "About DARPA," viewed July 25, 2019, available at <https://www.darpa.mil/about-U.S./about-darpa>.

[69] Robert D. Hof, "Lessons from Sematech," *MIT Technology Review*, July 25, 2011, available at <https://www.technologyreview.com/s/424786/lessons-from-sematech/>.

[70] Chrysler Corporation Loan Guarantee Act of 1979, P.L. 96-185, 96th Cong. (1980), available at <https://www.congress.gov/bill/96th-congress/hoU.S.e-bill/5860>.

[71] J.M. Bickley, "Chrysler Corporation Loan Guarantee Act of 1979: Background, Provisions, and Cost," R.40005, (Washington, D.C.: Congressional Research Service, 2008), available at <http://digitalcommons.ilr.cornell.edu/key_workplace/569>.

[72] Wikipedia, "Iridium Communications," viewed

July 17, 2019, available at <https://en.wikipedia.org/wiki/Iridium_Communications>.

[73] Secretary of Defense, "Determination Under Section 303 (a)(5) of the Defense Production Act for High Purity Beryllium Metal Production Program," October 12, 2005, available at <https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/Determination_of_the_Defense_Production%20Act_for_High_Purity_Beryllium_Metal_Production_Program.pdf>.

[74] Federal Reserve Bank of St. Louis, "Financial Crisis Timeline, 2007-2009," viewed on July 17, 2019, available at<https://www.stlouisfed.org/financial-crisis/full-timeline>; Department of the Treasury, "Investment in American International Group," available at <https://www.treasury.gov/initiatives/financial-stability/TARP-Programs/aig/Pages/default.aspx>.

[75] "American Recovery and Reinvestment Act of 2009," P.L. 111-5, 111th Congress (2009), available at https://www.congress.gov/bill/111th-congress/hoU.S.e-bill/1/text

[76] Farhana Hossain et al., "The Stimulus Plan: How to Spend $787 Billion," *The New York Times*, January 5, 2017, available at <https://www.nytimes.com/interactive/projects/44th_president/stimulU.S.>; Wayne Duggan, "What Happened to All the 'Shovel-Ready' Infrastructure Projects From the 2009 Stimulus Bill?", Benzinga, February 13, 2017, available at <https://www.benzinga.com/general/education/17/02/9036944/what-happened-to-all-the-shovel-ready-infrastructure-projects-from-t>.

[77] Steve Blank, "The Secret History of Silicon Valley," Stanford University, Computer History Museum Lecture, November 20, 2008, available at <https://www.youtube.com/watch?v=ZTC_RxWN_xo>.

[78] Office of the Secretary of Defense, Memo on Acquisition Policy for Commercial Products, July 14, 2000, available at <https://www.acq.osd.mil/dpap/docs/cotsreport.pdf>.

[79] Adam Stone, "To improve Military Networks, the Army Looks to Commercial Solutions," C4ISRNET, August 3, 2018, available at <https://www.c4isrnet.com/special-reports/military-it-modernization/2018/08/03/to-improve-military-networks-the-army-looks-to-commercial-solutions/>.

[80] Thomas Donahue, "Strategy Needed to Protect National Sovereignty of U.S. Telecommunications Backbone," *Military Cyber Affairs*, Vol. 3, Issue 2 (February 2018), available at<https://scholarcommons.U.S.f.edu/mca/vol3/iss2/4>; James Andrew Lewis, "Telecom and National Security," Center for Strategic & International Studies, March 18, 2018, available at <https://www.csis.org/analysis/telecom-and-national-security>.

[81] Defense Science Board, "Defense Applications of 5G Network Technology," Department of Defense, June 24, 2019, available at <https://www.acq.osd.mil/dsb/reports/2010s/5G_Executive_Summary_2019.pdf>.

[82] "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," R.43767 (Washington, D.C.: Congressional Research Service, 2018), available at <https://www.everycrsreport.com/reports/R43767.html>.

[83] Nokia Corporation, "Financial Report for Q4 and Full Year 2018," January 31, 2019, available at <https://www.nokia.com/about-U.S./news/releases/2019/01/31/nokia-corporation-financial-report-for-q4-and-full-year-2018/>; Ericsson, "Fourth Quarter and Full-year Report 2018," January 25, 2019, available at <https://www.ericsson.com/assets/local/investors/documents/financial-reports-and-filings/interim-reports-archive/2018/12month18-en.pdf>.

[84] Trefis Team, "Nokia's $16.6 Billion Acquisition of Alcatel-Lucent Explained," Forbes, April 16, 2015, available at <https://www.forbes.com/sites/greatspeculations/2015/04/16/nokias-16-6-billion-acquisition-of-alcatel-lucent-explained/#58334cc2605c>.

[85] Sijia Jiang, "China's Huawei to raise annual R&D budget to at least $15 billion," *Reuters*, July 26, 2018, available at <https://www.reuters.com/article/U.S.-huawei-r-d/chinas-huawei-to-raise-annual-rd-budget-to-at-least-15-billion-idU.S.KBN1KG169>; Habeeb Onawole, "Huawei join Samsung, Alphabet in Top 5 R&D investors for 2018," Gizmo China, January 2, 2019, available at <https://www.gizmochina.com/2019/01/02/huawei-join-samsung-alphabet-in-top-5-rd-investors-for-2018/>.

[86] Ruchi Gupta, "What Does Nokia Spend on Research and Development?", Market Realist, December 10, 2018, available at <https://marketrealist.com/2018/12/what-does-nokia-spend-on-research-and-development/>; Statista, "Nokia's Expenditure on Research and Development Since 1999," July 29, 2019, available at <https://www.statista.com/statistics/267821/nokias-expenditure-on-research-and-development-since-1999/>.

[87] Rochelle Toplensky and Alex Barker, "European Investment Bank: the EU's hidden giant," *The Financial Times*, July 15, 2019, available at <https://www.ft.com/content/940b71f2-a3c2-11e9-a282-2df48f366f7d>; Nokia, "Nokia lands EUR 500 million EU Financing for 5G research," August 27, 2018, available at <https://www.nokia.com/about-U.S./news/releases/2018/08/27/nokia-lands-eur-500-million-eu-financing-for-5g-research/>; Chris Kelly, "Canada to sign $40m 5G R&D deal with Nokia," Total Telecom, January 25, 2019, available at <https://www.totaltele.com/502006/

Canada-to-sign-40m-5G-RD-deal-with-Nokia>.

[88] Iain Morris, "Huawei Dwarfs Ericsson, Nokia on R&D Spend in 2017," Light Reading, April 3, 2018, available at < https://www.lightreading.com/artificial-intelligence-machine-learning/huawei-dwarfs-ericsson-nokia-on-randd-spend-in-2017/d/d-id/741944>; S. O'Dea, "Ericsson's Expenditure on Research and Development Worldwide from 2011 to 2018," Statista, May 6, 2019, available at <https://www.statista.com/statistics/566320/ericsson-research-and-development-expenses-worldwide/>; Corinne Reichert, "Ericsson Plans Continued 5G R&D as Net Loss Reduces to 700m SEK," ZDNet, April 20, 2018, available at <https://www.zdnet.com/article/ericsson-plans-continued-5g-r-d-as-net-loss-reduces-to-700m-sek/>.

[89] Jon Brodkin, "AT&T, facing $158 billion debt, to sell Puerto Rico network for $2 billion," Ars Technica, 9 October 2019, available at https://arstechnica.com/information-technology/2019/10/att-facing-158-billion-debt-to-sell-puerto-rico-network-for-2-billion/

[90] Mike Dano, "Huawei's Share of the Global Telecom Market Keeps Growing," Light Reading, 29 August 2019, available at https://www.lightreading.com/market-research/huaweis-share-of-the-global-telecom-market-keeps-growing/d/d-id/753768

[91] Edward White, "Inside Samsung's $116bn plan to overtake chip rivals," *Financial Times*, 22 July 2019, available at https://www.ft.com/content/85ebfa62-a2f8-11e9-a282-2df48f366f7d

[92] Song Jung-a, "Samsung closes US chip R&D unit," *Financial Times*, 5 November 2019, available at https://www.ft.com/content/8c773768-ffa3-11e9-b7bc-f3fa4e77dd47

[93] Wikipedia, "Nokia," viewed July 18, 2019, available at <https://en.wikipedia.org/wiki/Nokia>; Wikipedia, "Ericsson", viewed July 18, 2019, available at <https://en.wikipedia.org/wiki/Ericsson>.

[94] Samsung, "5G Core Vision," 2019, available at https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/5G_Core_Vision_Technical_Whitepaper.pdf

[95] "Ericsson Extends Global Supply Chain With Company's First Smart Factory in the U.S.," PRNewswire, June 26, 2019, available at <https://www.prnewswire.com/news-releases/ericsson-extends-global-supply-chain-with-companys-first-smart-factory-in-the-U.S.-300875136.html>; "Ericsson Increasing U.S. Investments To Support Accelerated 5G Deployments," Ericcson.com, August 10, 2018, available at <https://www.ericsson.com/en/press-releases/2018/8/ericsson-increasing-U.S.-investments-to-support-accelerated-5g-deployments>.

[96] Brian Womack, "Nokia's North Texas operations helping build T-Mobile's 5G network," Dallas Business Journal, July 30, 2018, available at <https://www.bizjournals.com/dallas/news/2018/07/30/nokias-north-texas-operations-helping-build-t.html>.

[97] Subcom, "Our Capabilities," viewed July 18, 2019, available at <https://www.subcom.com/>.

[98] "UbiquitoU.S. 5G Transport," Erricsson.com, viewed on July 18, 2019, available at <https://www.ericsson.com/en/networks/offerings/transport/5g-ready-transport>.

[99] William Lazonick and Edward March, "The Rise and Demise of Lucent Technologies,"*Business and Economic History On-line*, Vol. 9 (2011), available at <http://thebhc.org/sites/default/files/lazonickandmarch.pdf>.

[100] Nokia, "Nokia and Xiaomi sign Business Cooperation and Patent Agreements," July 5, 2017, available at <https://www.nokia.com/about-U.S./news/releases/2017/07/05/nokia-and-xiaomi-sign-bU.S.iness-cooperation-and-patent-agreements/>.

[101] *5G System Design: Architectural and Functional Considerations and Long-Term Research*, ed. Patrick Marsch et al. (United Kingdom: John Wiley & Sons Ltd., 2018), available at <https://onlinelibrary.wiley.com/doi/book/10.1002/9781119425144>.

[102] Steve McCaskill, "China Looking to Launch 6G by 2030," Techradar.pro, November 19, 2018, available at <https://www.techradar.com/news/china-looking-to-launch-6g-by-2030>.

[103] Matti Latva-aho, "Radio Access Networking Challenges Towards 2030" (Powerpoint Presentation, Oulu University, Finland, October 2018), available at <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201810/Documents/Matt_Latva-aho_Presentation.pdf>; "Discover How 6G will Change our Lives," University of Oulu, July 2019, available at <https://www.oulu.fi/6gflagship/>.

[104] Secretary of the Air Force, "Nuclear Command, Control and Communications," U.S. Air Force Instruction 13-550, April 16, 2019, <available at https://static.e-publishing.af.mil/production/1/af_a10/publication/afi13-550/afi13-550.pdf>.

[105] Erica D. Borghard and Shawn W. Lonergan, "The Overlooked Military Implications of the 5G Debate," Council on Foreign Relations, April 15, 2019, available at <https://www.cfr.org/blog/overlooked-military-implications-5g-debate>; U.S. Air Force Space Command, "Defense Satellite Communications System," March 22, 2017, available at <https://www.afspc.af.mil/About-U.S./Fact-Sheets/Display/Article/1012656/defense-satellite-communications-system/>; U.S. Air Force Space Command, "Advanced Extremely High Frequency System," March 22, 2017, available at <https://www.afspc.

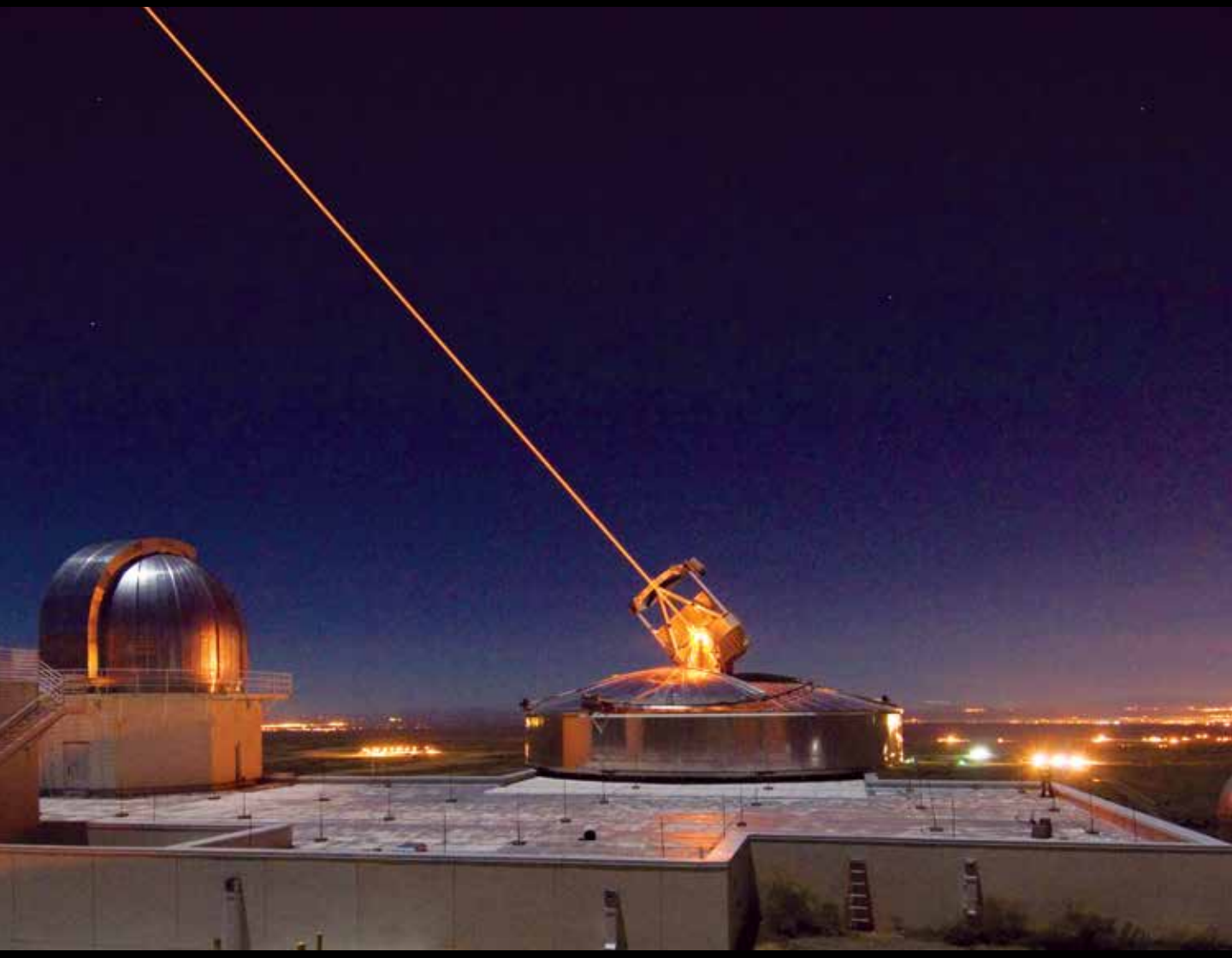
af.mil/About-U.S./Fact-Sheets/Display/Article/249024/advanced-extremely-high-frequency-system/>; U.S. Air Force Space Command, "Wideband Global SATCOM Satellite," March 22, 2017, available at <https://www.afspc.af.mil/About-U.S./Fact-Sheets/Display/Article/249020/wideband-global-satcom-satellite/>; U.S. Air Force Space Command, "Global Broadcast Service," March 22, 2017, available at <https://www.afspc.af.mil/About-U.S./Fact-Sheets/Display/Article/249021/global-broadcast-service/>; DM Chan, "Can commercial satellites cut U.S. defense costs?", Asia Times, July 15, 2019, available at <https://www.asiatimes.com/2019/07/article/can-commercial-satellites-cut-U.S.-defense-costs/>; Peter Barker, "The Challenge of Defending Subsea Cables," The Maritime Executive, March 20, 2018, available at <https://www.maritime-executive.com/editorials/the-challenge-of-defending-subsea-cables>.

[106] TeleGeography, "Submarine Cable Map," June 28, 2019, available at <https://www.submarinecablemap.com/#/>.

[107] "David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *The New York Times*, October 25, 2015, available at <https://www.nytimes.com/2015/10/26/world/europe/rU.S.sian-presence-near-undersea-cables-concerns-U.S..html>; Department of Homeland Security Analyst Exchange Program, "Threats to Undersea Cable Communications," Office of the Director of National Intelligence, September 28, 2017, available at <https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf>.

[108] Slava Solonitsyn, "Why U.S. Hardware Startups will Start Moving to China," Ruvento Ventures, March 19, 2017, available at <http://www.ruvento.com/news/2017/4/21/why-U.S.-hardware-startups-will-start-moving-to-china-1>; Richard Florida, "America is Losing Its Edge for Startups," City Lab, October 9, 2018, available at <https://www.citylab.com/life/2018/10/america-losing-its-edge-startups/572323/>.

[109] Zhou Xin, "Xi Jinping calls for 'New Long March in Dramatic Sign that China is Preparing for Protracted Trade War," South China Morning Post, May 21, 2019, available at <https://www.scmp.com/economy/china-economy/article/3011186/xi-jinping-calls-new-long-march-dramatic-sign-china-preparing>.



The Sodium Guidestar at the Air Force Research Laboratory Directed Energy Directorate's Starfire Optical Range. Researchers with AFRL use the Guidestar laser for real-time, high-fidelity tracking and imaging of satellites too faint for conventional adaptive optical imaging systems. The SOR's world-class adaptive optics telescope is the second largest telescope in the Department of Defense. (Courtesy photo)

Directed Energy Weapons Are Real . . . And Disruptive

By Henry "Trey" Obering, III

In the 1951 science fiction film, "The Day the Earth Stood Still," powerful ray guns are shown vaporizing rifles and even tanks. In the Star Wars movies, a wide variety of directed energy weapons are depicted, from handheld light sabers to massive, spaceship-mounted laser cannons.

What exactly is a directed energy weapon? Are these weapons still science fiction, lab experiments, or are they real? How can they be used and how disruptive can they be? What are the challenges and next steps? This article will examine answers to these questions.

What are Directed Energy Weapons?

According to DOD's Joint Publication 3–13 Electronic Warfare, directed energy (DE) is described as an;

> *umbrella term covering technologies that produce a beam of concentrated electromagnetic energy or atomic or subatomic particles. A DE weapon is a system using DE primarily as a direct means to disable, damage or destroy adversary equipment, facilities, and personnel. DE warfare is military action involving the use of DE weapons, devices, and countermeasures to either cause direct damage or destruction of adversary equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum (EMS) through damage, destruction, and disruption.*[1]

DE weapons include high-energy lasers, high-power radio frequency or microwave devices, and charged or neutral particle beam weapons.[2] Microwaves and lasers are both part of the electromagnetic spectrum, which includes light energy and radio waves. The distinction between them is the wavelength/frequency of the energy. While they are both part of the electromagnetic spectrum, laser and microwave weapons operate very differently and have very different effects.

Think of the difference between a laser pointer and a flashlight. The laser light is coherent in a single color, and the flashlight is broad-spectrum light. Because of its coherence, laser light can stay concentrated for very long distances—even thousands of miles into space. But with laser weapons, instead of thinking in terms

Lieutenant General Henry "Trey" Obering, III, USAF (ret.), is an Executive Vice President and Directed Energy Lead at Booz Allen Hamilton and the former director of the Missile Defense Agency.

of a laser pointer, the mental image should be more like a powerful, long-range blowtorch!

Lasers can be categorized as gas, solid state, or a hybrid of the two. The lasers on the current path to weaponization include solid state combined fiber and crystal slab as well as hybrid lasers. Fiber lasers are lasers in which the active medium being used is an optical fiber that has been doped in rare elements, most often Erbium.[3] Slab lasers represent one class of high-power solid-state lasers in which the laser crystal has the form of a slab.[4] Hybrid lasers such as a diode pumped alkali laser use a combination of trace gas with semiconductor diode arrays for even higher power and efficiency.[5]

The destructive power of directed energy weapons (their lethality) derives from the amount of energy transferred to the target over time. This concentrated energy can have effects across the entire spectrum from non-lethal to lethal. For example, lasers can cut through steel, aluminum, and many other materials in a matter of seconds. They can be very effective in causing pressurized vessels to explode such as missile propellant and oxidizer tanks. They can destroy, degrade or blind many other systems that contain sensors and electronics. For high energy lasers, lethality depends on the power output of the laser, the purity and concentration of the light (beam quality), the target range, the ability to keep the laser on the target aimpoint (jitter control and tracking), and the atmospheric environment the laser traverses to the target. In this last factor, the frequency of the laser and the engagement altitude will have a significant impact on how much the atmosphere effects the laser's lethality. Laser energy can be generated as a continuous wave or in pulses, which also influences its lethality. High-energy lasers (HEL) can range from a few kilowatts to megawatts of average power.

High-power microwave (HPM) and high-power millimeter wave weapons emit beams of electromagnetic energy typically from about 10 megahertz to the 100 gigahertz frequency range. Like lasers, HPM weapons can operate in a pulsed or continuous manner and are classified using "peak" or "average" power respectively. Most HPM systems are based on short pulses of radiofrequency (RF) energy, for which peak power is the important metric. The antenna gain of the weapon system is also very important, and when combined with the power of the RF source, yields the Effective Radiated Power (ERP) of the weapon. Depending on the particulars of the weapon, and how it is used, ERP levels can reach into the hundreds of gigawatts or higher. For continuous wave systems, which use high average power to effect targets, levels are typically from 50 to 100s of kilowatts up to several megawatts of power. The power levels are driven by prime power generation limitations, and ERP's depend on the antenna design and aperture (i.e., size).[6]

Almost everyone has probably experienced the "lethality" of a microwave device when they inadvertently put a metal object into a kitchen microwave oven and watched the "sparks fly." This same energy can be applied at higher powers for weapon effects. There are numerous pathways and entry points through which microwave energy can penetrate electronic systems. If the microwave energy travels through the target's own antenna, dome, or other sensor opening, then this pathway is commonly referred to as the "front door."[7] On the other hand, if the microwave emissions travel through cracks, seams, trailing wires, metal conduits, or seals of the target, then this pathway is called the "back door."[8]

In the weapons version, the microwave energy effects or lethality depends on the power and range to target, but the energy beams tend to be larger and not as sensitive to jitter as is the case for the high energy lasers. HPM lethality can be affected by atmospheric conditions as well, but to a much lesser degree than high-energy laser (HEL) weapons. HPM weapons lethality is typically described in terms of their ability to deny, degrade, damage or destroy a target's capabilities.

The term "deny" is defined as the ability to eliminate the enemy's ability to operate without inflicting harm on the system. A microwave weapon can achieve this result by causing malfunctions within certain relay and processing circuits within the enemy target system. For example, the static and distortion that high voltage power lines have on a car radio causes no lasting damage to the radio after the car leaves the area. Thus, the "deny" capability is not permanent because the affected systems can be easily restored to their previous operational condition.

The meaning of "degrade" is to remove the enemy's ability to operate and to potentially inflict minimal injury on electronic hardware systems. Examples of this capability include signal overrides or insertion, power cycling (turning power on and off at irregular intervals) and causing the system to "lock-up." These effects are not permanent because the target system will return to normal operation within a specified time, which obviously varies according to the weapon. In most cases, the target system must be shut off and restarted, and may require minor repairs before it can operate normally again.

The idea of "damage" is to inflict moderate injury on enemy communications facilities, weapons systems, and subsystems hardware, and to do so in order to incapacitate the enemy for a certain time. Examples include damaging individual components, circuit cards, or the "mother boards" in a desktop computer. This damage may create permanent effects depending upon the severity of the attack and the ability of the enemy to diagnose, replace, or repair the affected systems.

Finally, the concept of "destroy" involves the ability to inflict catastrophic and permanent injury on the enemy functions and systems. In this case, the enemy would be required to totally replace entire systems, facilities, and hardware if it was to regain any degree of operational status.[9]

In addition to being able to scale effects on a target, directed energy weapons have inherent attributes that are attractive to the warfighter. These include:

- speed of light engagement which makes responsiveness and tracking much faster than kinetic weapons;
- deep shot magazines which are only limited by the electrical power supplied to and re-generated by the system;
- "stealth-like" performance (quiet and invisible beams) that are hard to detect or intercept;
- precision targeting for both lethal and non-lethal applications; and
- low-cost per shot compared to traditional munitions.

Directed energy weapons have been in development for decades in our nation's research and development organizations, national laboratories and industry. So how close are they to becoming weaponized?

Are Directed Energy Weapons Still Science Fiction, Lab Experiments or Ready for the Warfighters?

In early versions of laser weapons, the light was generated by chemical reactions. Between 2000–05, a prototype chemical laser successfully destroyed 46 rockets, artillery shells and mortar rounds in flight during field tests. However, these lasers were generally large and heavy. In fact, the megawatt-class Airborne Laser developed in the late 1990s and early 2000s required an entire 747 aircraft to hold the equipment. Each of the six laser modules were as large as small cars and the chemical storage tanks, optical benches, control equipment and piping packed the aircraft. In 2010, the Airborne Laser shot down two missiles (both solid and liquid propelled) in their boost phase during flight testing which demonstrated

the lethality of the laser against missile targets. We proved that the technology could be effective, but its size, weight, and power (SWaP) requirements made the laser weapons impracticable to field.

Today, solid state electrical (including fiber) and hybrid lasers are being developed that are much lighter and smaller. The combination of technology advancements improving lethality and reducing SWaP in high energy laser technology and the advent of threats such as hypersonic weapons for which kinetic solutions are problematic has resulted in high energy lasers and directed energy weapons more generally being pursued vigorously across the services consistent with the *National Defense Strategy*.[10]

In recent years the U.S. Navy deployed a 30kW class solid state laser weapon system (LaWS) prototype on the Afloat Forward Staging Base, USS *Ponce*. It was capable of damaging or destroying fast attack boats, unmanned aerial vehicles and was used for intelligence, surveillance, and reconnaissance (ISR). When the LaWS was being integrated onto the ship, the designers and developers envisioned that it would be used several hours a day. It turned out that during its three-year deployment, from 2011–14, it was used nearly around the clock in its ISR mode.

Because of the strategic imperative to protect U.S. carrier battlegroups to enable us to project power, the U.S. Navy is following this prototyping effort with a much broader "Navy Laser Family of Systems" or NLFoS program, which will put the Navy on a path to develop and deploy lasers ranging from low power laser "dazzlers" to much higher power lasers capable of destroying anti-ship and high-speed cruise missiles. Examples of NLFoS weapons include: a 60kW laser called HELIOS (High Energy Laser with Integrated Optical-dazzler and Surveillance) expected to be deployed by 2021 that will be capable of burning through small boats and shooting down drones; the SSL–TM (Solid State Laser–Technology Maturation system), which will eventually be a 150kW laser weapon on the LPD–27 amphibious ship; and the ODIN (Optical Dazzling Interdictor, Navy) that will also go on a destroyer.[11]

The U.S. Army has also been moving out aggressively in developing and deploying directed energy weapons as part of its Air and Missile Defense modernization priority. Within that priority area, the Army is focused on the use of high energy lasers to provide Indirect Fire Protection Capability (IFPC) and Maneuver—Short-Range Air Defense (M-SHORAD). The Army's Rapid Capabilities and Critical Technologies Office is now asked to make DE technology available to the warfighters as quickly as possible. Building on the Army's DE efforts during the past 5 to 7 years, the Rapid Capabilities and Critical Technologies Office (RCCTO) is committed to fielding 50kW lasers on four Strykers (eight wheeled armored fighting vehicles), delivering a residual combat capability at the Platoon level as part of the M-SHORAD mission in support of a Brigade Combat Team.

Building a Stryker with a 50kW laser is a follow-on to the 5kW laser the Army tested on the vehicle just a year ago in Germany at the Joint Warfighting Assessment and related efforts. *DefenseNews* in their coverage of the March 2018 Booz Allen Hamilton/CSBA Directed Energy Summit in Washington highlighted the remark by Colonel Dennis Wille, the Army G3 strategic program chief for U.S. Army Europe, that over the weekend the 2nd Stryker Cavalry Regiment (supported by the 7th Army Training Command and the Fires Center of Excellence at Fort Sill, Oklahoma) had conducted a live-fire engagement of the 5kW Mobile Expeditionary High-Energy Laser demonstrator at the Grafenwoehr Training Area, Germany. This is just the beginning of a plan to deploy 50kW lasers on four of its Stryker vehicles over the next few years for operational use.[12]

A fire support noncommissioned officer with 4th Division Artillery, 4th Infantry Division, who participated in the testing of a 2kW version of the laser

vehicle at Fort Sill, Oklahoma against unmanned drones was quoted in a February 28, 2018 *Army Times* article as saying, "It was extremely efficient, I was able to bring them down as [fast as] they were able to put them up."[13]

The Army used Navy-, and Air Force- developed HPM weapons during recent conflicts to counter improvised explosive devices (IEDs). These devices have also been demonstrated to stall or damage car, truck, or boat motors. This capability would be very useful at checkpoints or for stopping escaping vehicles.

In 2017, the Air Force Secretary and Chief of Staff signed the DE Flight Plan outlining the path ahead for the Air Force to develop and deploy both high-energy lasers and high-power RF weapons for its aircraft. This plan includes a program which aims to test high energy lasers on aircraft against surface to air and air to air missile threats. Similar to the Army's RCCTO and the Navy's Accelerated Acquisition (AA) Process, the Air Force is leveraging both Air Force Research Laboratory's DE Directorate and Air Force Strategic Development Planning and Experimentation Office to expedite delivery of capabilities to address key capability gaps identified in the DE flight plan: Forward Base Defense, Precision Strike, and Aircraft Self-Protect. In addition, the Air Force has partnered with the Navy in the development of a high-power RF weapon called High-power Joint Electromagnetic Non-Kinetic Strike (HiJENKS) capable of attacking electronics, communications and computer networks.

The Air Force also recently demonstrated the ability of an HPM weapon to bring down multiple drones in testing at White Sands Missile Range in New Mexico, according to a recent Military.com article:

> *"After decades of research and investment, we believe these advanced directed-energy applications will soon be ready for the battlefield to help protect people, assets and infrastructure." Thomas Bussing, Raytheon Advanced Missile Systems vice president, said in a news release accompanying the announcement. The release noted the HPM and HEL systems engaged and defeated "dozens of unmanned aerial system targets" during the exercise.*[14]

But by far, the most ambitious program underway in DOD is being led by the Missile Defense Agency (MDA). It is developing a very high-power laser capable of being eventually deployed on a space-based platform to target missiles during their boost/ascent/midcourse phase. This laser would be megawatt class and have a range of hundreds of miles.

The first step in this endeavor is underway with funding for laser scaling and beam quality improvements for both combined fiber lasers as well as hybrid lasers such as the diode pumped alkali laser or DPALS. These lasers, combined with significant improvements in computational power, represent dramatic advances in technology over those used in the Airborne Laser program. The

The High Energy Laser Mobile Demonstrator, or HEL MD, is the result of U.S. Army Space and Missile Defense Command research. (Army photo)

laser diodes, fiber amplifiers, battery and power management, thermal control, and optical systems are also much more advanced.

The United States will soon be reaching the point where it can generate a megawatt of power in a size, weight, and volume capable of being put on a high-altitude aircraft or space-based platform. As DOD works to develop and incorporate these technologies, much of the work should be collaborative, such as improvements in materials, power generation, thermal control, etc. to reduce size, weight, and power required to operate these weapons. However, the wide variety of missions, platforms, and implementation environments necessitates continued service-differentiated development activities. This also includes fundamental differences such as the wavelength of the lasers and the beam quality required for success.

For example, a Navy ship-to-air laser will have different requirements than an Air Force air-to-air system, which will have different requirements than a space-based missile defense system and therefore different technological considerations. Discrete, mission-aligned efforts will maintain our pace of development in the race to get these technologies to the field.

How Can They Be Used and How Disruptive Can They Be?

Some applications of directed energy weapons to solve today's challenges have already been described, such as stopping swarms of small adversary boats which have been harassing U.S. ships in international waters, or stopping vehicles carrying improvised explosive devices at a safe distance from U.S. personnel. As another example, high energy lasers could be used to protect forward-deployed troops and bases from attacks by swarms of unmanned aircraft carrying explosive devices.

But let us broaden these applications somewhat. In addition to the nuclear ballistic missile threat posed by North Korea, which can be defended by U.S. missile defense systems, there is a North Korean threat which cannot be defended against today . . . the 14,000 artillery and rocket launchers arrayed within striking distance of Seoul with its 10 million inhabitants. Imagine how much the geopolitical calculus would change on the peninsula if a layered, integrated system of high energy lasers and high-power microwave weapons was deployed to defend against these threats.

Turning to the air, the United States spent billions of dollars to develop and deploy stealth technology for its fighters and bombers to avoid radar detection and being targeted by surface to air missiles. What if the United States could deploy effective anti-missile lasers on its' aircraft to defeat any missile(s) fired at them? In effect, the United States would have provided "stealth-like" capability to entire fleets of aircraft.

In a much more dramatic application, the recently released *Missile Defense Review* (MDR), the first update to *U.S. Missile Defense Strategy* in nearly a decade, delivers a visionary plan to protect the United States from ever-intensifying threats around the world. For example, the MDR proposes that the Missile Defense Agency study the potential to develop and field space-based lasers to intercept ballistic missiles.[15]

Space-based lasers would have a profound impact on the U.S. ability to defend and if necessary, fight in space. Not only could they be used to defend against ballistic missiles in the boost/ascent and midcourse phase, but they could also be used to defend critical space-based assets against enemy anti-satellite attack.

Directed energy weapons could also play a key role in defending against what has been described as the number one threat to the United States by the Undersecretary of Defense for Research and Engineering Dr. Mike Griffin—hypersonic weapons. He has pressed for the development of hypersonic weapons by the United States as well as a defense

against them. In a March 6, 2018 speech, said, "I'm sorry for everybody out there who champions some other high priority, some technical thing; it's not that I disagree with those," he told the room, "But there has to be a first, and hypersonics is my first."[16]

There are two types of hypersonic weapons, boost glide and air-launched high-speed cruise missiles. Boost glide weapons are launched atop ballistic missiles then released to glide to the target. The air-launched uses scramjets or rockets to power it throughout flight. These high-speed missiles fly at Mach 5 (five times the speed of sound) and greater. They can not only achieve these speeds but can maneuver at them as well including varying trajectories, headings and altitudes. Therefore, currently deployed defenses against ballistic missiles will not be effective in defending against these non-ballistic threats. There is no "silver bullet" defense against these weapons and in fact there will have to be an architectural approach in defending against them, but directed energy weapons can potentially play a major role.

Since these weapons maneuver, the United States needs to be able to precisely track the hypersonic missile throughout its entire flight or "birth to death." The only cost-effective way to accomplish this is using space-based satellites. Developing hypersonic interceptors will also be an option in the U.S. defense architecture. But there is a rule of thumb that states that an interceptor needs to be capable of three times the speed of the target it is defending against to be able to maneuver to destroy it. So hypersonic kinetic interceptors would have to be capable of achieving speeds of Mach 15 and higher.

One of the greatest attributes of directed energy weapons is that they operate at the speed of light. So, for a hypersonic weapon that is travelling at 25 times the speed of sound, a high- energy laser can engage it at roughly 35,000 times its speed. This makes targeting and tracking easier as well. Space-based high energy lasers could be brought to bear especially in the boost/ascent phase of boost glide hypersonic missiles where a high-energy laser could destroy the vehicle early in its trajectory. At the speeds that these hypersonic missiles fly, they have vulnerabilities which could be exploited by directed energy weapons. Therefore, HELs and HPMs could also play a role in the midcourse/terminal phase of both types of hypersonic missile flight.

Directed energy weapons are no longer just science fiction. They are real and are maturing rapidly. In the next several years, the U.S. Army, Navy and Air Force all plan to develop and field these weapons at an increasing pace. They will be deployed on land vehicles, aircraft, helicopters, and ships.

Even the most conservative market projections for directed energy weapons indicate nearly $30 billion being spent by the United States during the next ten years. They are not the answer to all the challenges, and will not replace kinetic weapons, but they are an essential adjunct to countering specific threats and providing dominance in land, air, sea, and space. The United States has the technology, the resources, the talent, and the infrastructure to develop and deploy directed energy weapons to meet today's and tomorrow's emerging threats.

The only question is whether the United States and its allies will achieve that dominance before an adversary does.

What Are the Challenges and Next Steps?

The United States has come a very long way in the development of directed energy weapon capabilities and is now at a critical juncture. The technology is maturing rapidly, threats are emerging which directed energy can almost uniquely address, and the warfighters are signaling their support.

However, as with the development of any unprecedented military capability, there are risks, challenges and limitations involving their cost, schedule and performance. In the case of directed

energy weapons, there has been significant risk reduction which has been accomplished over several decades. Examples of this cited earlier included the Airborne Laser, the Navy's LaWS program, and others. However, risks, challenges and limitations remain.

For example, atmospheric conditions such as turbulence, haze, clouds, etc. can affect a laser's performance but there are ways to address these phenomena. First, the choice of a laser's wavelength can help to mitigate the affect because different laser wavelengths perform much better in the atmosphere than others. And of course, lasers employed at higher altitudes or in space would have very little to no atmospheric affects.

In addition, a technique known as "adaptive optics" has been developed for many years. In this case, the laser weapon system would sense the atmospheric conditions to the target, then using fast steering mirrors, it would deform the main laser beam as it leaves the weapon to use the atmosphere to the target much like the lens of a pair of glasses to refocus the beam on the target. Increasing laser power and improving the beam quality can also help to mitigate atmospheric effects in many cases.

Challenges remain in terms of the size, weight and power input requirements of today's laser systems, especially in the thermal control and power management subsystems. But again, there are major advances in these areas being made especially with the technology that has been developing in the electric car industry.

When using laser weapons, the warfighters will need new situational awareness and battle management tools because of the potential long-range effects to avoid friendly systems fratricide. But again, advances in computational power coming out of the gaming industry (such as graphics processing units) and artificial intelligence coming from autonomous automobile development can be instrumental in providing these needed capabilities.

While the development costs of directed energy systems can be high, there are several factors in play which can reduce these costs or at least provide better return on the investment over the life cycle. For example, as mentioned earlier, directed energy weapons development can take advantage of progress being made in commercial industry around processors, power generation and management and even lasers subsystems themselves.

In addition, the "cost per shot" of a directed energy weapons could be orders of magnitude less expensive than current kinetic weapons. Consider that today the United States will launch kinetic interceptors at an incoming threat warhead that cost tens of millions of dollars and multiple interceptors are fired for maximum probability of success. Compare that to a high energy laser which could kill multiple threat missiles with a single "magazine" charge for a tiny fraction of the cost. In addition, while you are firing on one power source, you can be charging another for near continuous operation.

More importantly, peer and near-peer nations are developing these weapons at an alarming rate. The United States must realize that it has to resource the development and fielding of these capabilities. The United States cannot allow itself to fall behind in yet another area of warfighting as has happened in hypersonics.

To maximize the United States' ability to field DE weapons, here is a ten-part approach to get us going in the right direction:

1. **Power Scaling and Improved Beam Quality.** DOD should significantly scale up laser power and improve beam quality; as well as develop higher power compact microwave weapons. The pace of maturing these capabilities is not "technology limited;" it is "funding limited," therefore the United States should ensure that funding for directed energy weapon development supports the needed developments. Levels of $3 billion or above per year should be maintained.

2. **SWaP Reduction.** The United States should accelerate efforts to reduce the size, power input, weight, and cost requirements of these weapons. Since the most demanding size, weight and power inputs requirements are in the missile defense arena, MDA laser programs should be fully funded to increase laser power levels for high-altitude and space-based applications.
3. **Warfighter Tactical Decision Aids.** DOD should provide warfighters with tactical decision aids to ensure they know how and when to use these weapons. This will go far toward instilling confidence in the warfighters that these weapons will be effective in combat against multiple threats. These aids would include a guide to their effectiveness, similar to what the Joint Munitions Effectiveness Manual does for kinetic weapons.
4. **Lethality.** The Office of the Secretary of Defense should fund a program to focus broadly on improving understanding of microwave and laser weapon lethality. While a tremendous amount of work has been done, DOD should also conduct further research to enhance understanding of laser and high-power microwave lethality and reliability across an increasing range of weather and atmospheric conditions. This research should also focus on minimizing any collateral damage.
5. **Accelerated Acquisition.** DOD should accelerate acquisition of DE capabilities using non-traditional practices. According to Griffin, at the 9th Annual Defense Programs Conference in March 2018, DOD takes an estimated 16.5 years to bring new technologies from statement of need to deployment. But there are several examples where the timelines have been dramatically shortened such as the Navy's Rapid Prototyping Experimentation and Demonstration (RPED) program for mission-critical capabilities and the use of specialized acquisition authorities by the MDA. DOD should use such accelerated processes for DE development and deployment.
6. **Long-term Commitment.** DOD must signal a long-term commitment to directed energy, so the industrial base will know there will be a market for its products in the coming years. In doing so, DOD should prepare, and encourage, the industrial base to support the rising need for first-, second-, and third-tier suppliers.
7. **Testing Infrastructure.** DOD should provide the needed testing infrastructure for directed energy weapons especially as they can achieve longer and longer ranges. This needs to include rapid airspace deconfliction capabilities.
8. **Increased Collaboration.** All parties involved in directed energy development should continue to talk to each other. Significant progress has been made in communication and collaboration across the technical community through their involvement in the Directed Energy Professional Society (DEPS) and by the HEL Joint Technology Office. DOD needs to better articulate its requirements for deployable lasers. But also, the industrial base must interface better with DOD and its leadership to increase understanding of innovative laser weapon capabilities.
9. **Training.** DOD must also prioritize warfighter training. There is currently no established directed energy training pipeline; that is because laser and microwave weapons have no formal programs of record (PORs). Once the PORs are set up, training must follow. To assist in establishing PORs, DOD should encourage wargames and operational analysis to investigate and better articulate the battlefield benefits of lasers.
10. **Command and Control.** DOD should adapt command-and-control functions to address

rapidly evolving threats, such as hypersonics, to reduce the engagement times of defensive systems. Very short engagement timelines will likely necessitate the incorporation of artificial intelligence capabilities to help the United States leverage the speed-of-light engagement that directed energy weapons offer.

These are steps to take to bring directed energy prototype systems to the warfighters. The brave men and women who confront dangerous threats across all physical domains—land, air, sea, and space—need nothing less than the world's most promising new capabilities to protect U.S. national security. Adversaries are not waiting to develop directed energy weapons. Neither should we. PRISM

Notes

[1] Department of Defense Joint Publication 3-13.1, Electronic Warfare (Washington, DC: Department of Defense, 2012).

[2] According to the Lawrence Livermore Laboratory,

> *The word "laser" is an acronym for light amplification by stimulated emission of radiation. Laser light is created when the electrons in atoms in special glasses, crystals, or gases absorb energy from an electrical current or another laser and become "excited." The excited electrons move from a lower-energy orbit to a higher-energy orbit around the atom's nucleus. When they return to their normal or "ground" state, the electrons emit photons (particles of light). These photons are all at the same wavelength and are "coherent," meaning the crests and troughs of the light waves are all in lockstep. In contrast, ordinary visible light comprises multiple wavelengths and is not coherent.*

Additional information on "How Lasers Work," is available on the Lawrence Livermore National Lab website, <https://lasers.llnl.gov/education/how_lasers_work>.

[3] "How a Fiber Laser Works," SPI Lasers International website, available at <https://www.spilasers.com/industrial-fiber-lasers/how-fiber-lasers-work/>.

[4] "Slab Lasers," RP Photonics Encyclopedia website, available at <https://www.rp-photonics.com/slab_lasers.html>.

[5] Ibid.

[6] David Stoudt, Ph.D., Electrical Engineering, private communication.

[7] David M. Sowders et al., "High Power Microwave (HPM) and Ultrawideband (UWB): A Primer on High Power RF," PL-TR-95-1111, Special Report, Phillips Laboratory, March 1996, 76.

[8] Ibid, 79.

[9] Eileen Walling, "High Power Microwaves, Strategic and Operational Implications for Warfare," Occasional Paper no. 11, Air War College Center for Strategy and Technology, May 2000.

[10] Department of Defense, *The National Defense Strategy 2018* (Washington D.C.: Office of the Secretary of Defense, 2018).

[11] Megan Eckstein, "Navy to Field High-Energy Laser Weapon, Laser Dazzler on Ships This Year as Development Continues," USNI News, May 30, 2019.

[12] Jen Judson, "U.S. Army Successfully Demos Laser Weapon Stryker in Germany," DefenseNews.com, March 21, 2018, available at < https://www.defensenews.com/land/2018/03/21/us-army-successfully-demos-laser-weapon-on-stryker-in-europe/>.

[13] Todd South, "Soldiers in Europe are now Using Lasers to Shoot Down Drones," ArmyTimes.com, February 8, 2018, available at < https://www.armytimes.com/news/your-army/2018/02/28/soldiers-in-europe-are-now-using-lasers-to-shoot-down-drones/>.

[14] Oriana Powlyk, "Raytheon Directed-Energy Weapons Down Drones in Air Force Demonstration," Military.com, May 1, 2019, available at <https://www.military.com/daily-news/2019/05/01/raytheon-directed-energy-weapons-down-drones-air-force-demonstration.html>.

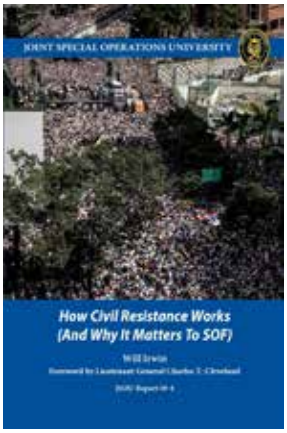
[15] Office of the Secretary of Defense, "Missile Defense Review," January 2019, available at < https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf>.

[16] R. Jeffrey Smith, "Hypersonic Missiles Are Unstoppable and They're Starting a New Global Arms Race," *New York Times Magazin*e, June 19, 2019.

Joint Special Operations University (JSOU) Press

JSOU Press publications are accessible online via the USSOCOM Research Library web site.
https://jsou.libguides.com/jsoupublications

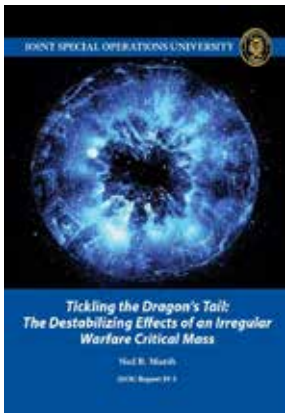
HOW CIVIL RESISTANCE WORKS (AND WHY IT MATTERS TO SOF)



By Will Irwin

Mr. Will Irwin reminds us in this extremely timely and well-written monograph, as John F. Kennedy observed more than a half century ago, that those who make peaceful revolution impossible will make violent revolution inevitable. Million man protest marches in Hong Kong, riots and rebellion in Caracas, continued rumors of widespread discontent in Tehran, sabotage in the face of unspeakable brutality in North Korea, sectarian civil war in Syria, and the unrelenting assault on liberal democracy by the dictatorial regime in Moscow—the headlines of today have their seeds in the inherent fear of tyrants. It is that fear on which America must capitalize and be prepared to use to our advantage. These disturbances reveal the critical role that America's special warfare units play in the contemporary era of nation state competition and conflict, for it's their own people that our enemies fear most. Will Irwin's monograph is a timely and important contribution to what will eventually become canon for the American Way of Irregular War and the basis for the professional military education of its uniformed and civilian irregular warfare practitioners.

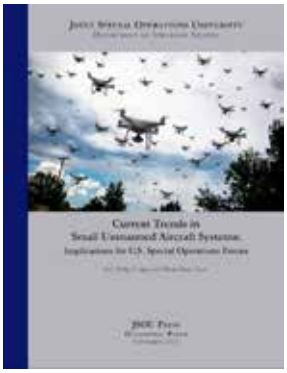
TICKLING THE DRAGON'S TAIL: THE DESTABILIZING EFFECTS OF AN IRREGULAR WARFARE CRITICAL MASS



By Ned B. Marsh

Lieutenant Colonel Ned Marsh wrote this monograph while attending the U.S. Army School of Advanced Military Studies. He proposes that over time a metaphorical critical mass constructed of global irregular warfare (IW) actors, state and non-state, has developed. The core is now active and exists within an enabling contemporary environmental structure. State warfare hegemony has decreased conventional competition and increased asymmetrical strategies. The result of this has been the emergence of IW as a prominent strategy and a self-propagating chain reaction of IW activity. This activity is releasing increasingly dangerous levels of destabilizing effect. This monograph reviews IW theory and history, and describes the contemporary operational paradigm. It analyzes the effect of cumulative IW activity and discusses prescriptive approaches to the problem. It concludes that, if stability is an objective, then counter-IW must be holistically undertaken with strategies to reduce conventional warfare competition.

CURRENT TRENDS IN SMALL UNMANNED AIRCRAFT SYSTEMS: IMPLICATIONS FOR U.S. SPECIAL OPERATIONS FORCES



By J. Philip Craiger and Diane Maye Zorri

In this new occasional paper, Dr. J. Philip Craiger and Dr. Diane Maye Zorri explore current trends in small unmanned aircraft systems (sUAS) technology and its applications to Special Operations Forces (SOF). The paper begins with analysis of the definition and classification of sUAS, their major applications, and characteristics. The authors then present sUAS military applications, threats, current/future threat scenarios, and counter-sUAS capabilities and technology. The authors conclude with a look at the five-year trends in sUAS to include cyber-enabled counter-sUAS. Setting the stage in their introduction the authors state, "As armed forces around the world continue to invest in research and development of sUAS technologies, there will be tremendous potential to revolutionize warfare, particularly in context of special operations."

Neuron cells system - 3d rendered image of Neuron cell network on black background. Hologram view interconnected neurons cells with electrical pulses.

Redefining Neuroweapons

Emerging Capabilities in Neuroscience and Neurotechnology

By Joseph DeFranco, Diane DiEuliis, and James Giordano

As global conflicts assume increasingly asymmetric and "gray zone" forms, the ability to employ current and newly developing techniques and tools of neurocognitive science to manipulate human thought and behavior must be viewed as a present and increasing challenge.[1] Ongoing developments in neuroscience and technology (neuroS/T), which trend toward 5- to 10-year trajectories of progression, make the brain sciences valid, viable, and of growing value for operational use in warfare, intelligence, and national security (WINS) applications. Illustrative of this progress are a series of U.S. Government assessments of such capabilities. A 2008 report by the ad hoc Committee on Military and Intelligence Methodology for Emergent Neurophysiological and Cognitive/Neural Science Research in the Next Two Decades claimed that neuroS/T was not sufficiently mature to enable operational employment in WINS. However, a subsequent report by this same committee in 2014 noted that advancements enabled several domains of neuroS/T to be capable and operationalizable for WINS. This was substantiated by a number of nations' increased interest in, and consideration and use of, neurocognitive methods and tools for military and intelligence purposes.[2] Indeed, neuroS/T can be employed as both "soft" and "hard" weapons in competition with adversaries. In the former sense, neuroS/T research and development can be utilized to exercise socio-economic power in global markets, while in the latter sense, neuroS/T can be employed to augment friendly forces' capabilities or to denigrate the cognitive, emotive, and/or behavioral abilities of hostiles. Furthermore, both "soft" and "hard" weaponized neuroS/T can be applied in kinetic or non-kinetic engagements to incur destructive and/or disruptive effects.[3]

Historically, biochemical weapons have included incapacitating or lethal agents such as nerve gas, irritants, vesicants, and paralytics. Numerous examples of such weapons can be drawn from World War I to the present. As shown in Table 1, various forms of neuroS/T have become available, and radical leveling and emerging developments in the brain sciences fortify and add to this current palette of weaponizable tools.

Mr. Joseph DeFranco is a Donavan Group fellow at U.S. Special Operations Command. Dr. Diane DiEuliis is a senior research fellow at National Defense University, and Dr. James Giordano is professor of neurology and biochemistry, chief of the Neuroethics Studies Program, and co-director of the O'Neill-Pellegrino Program in Brain Science and Global Law and Policy at Georgetown University Medical Center.

Table 1. Current and Near-term NeuroS/T Approaches to Optimizing Human Performance in WINS

Current and Near-term neuroS/T approaches to optimizing human performance in WINS	
Pharmacological Agents	• Stimulants (e.g., amphetamines) • Eugeroics (e.g., modafinil) • Non-stimulant cognitive enhancers (e.g., ampakines) • Other nootropics (e.g., racetams) • General positive mood-altering agents (e.g., monoamine reuptake inhibitors and beta-blockers)
Neurotechnological Devices	• EEG-based neurofeedback • Transcranial neuromodulation • Brain-machine-interfaces
Intelligence Applications	• Physiomimetic computing • Systems with automated learning capabilities • Modeling cognition and other neural systems to create new analysis tools • "Big data"–based processing of individual and group behavioral/semantic responses to narratives, semiotics, etc.
Current and near-term neuroS/T approaches to influencing/impairing opponents	
Neuropharmacological Agents	• Tranquilizing agents (e.g., benzodiazepines, barbiturates, etc.) • Mood-altering agents (e.g., monoamine agonists) • Affiliative agents (e.g., MDMA, oxytocin) • Dissociative agents (e.g., ketamine, phencyclidine) • Psychedelics/hallucinogens (e.g., LSD, psilocybin, tryptamine derivatives) • Cholinergic agents (e.g., pilocarpine, physostigmine, sarin)
Neuromicrobial Agents	• Viruses (e.g., Togaviridae, Flaviviridae) • Bacteria (e.g., Bacillis anthracis, Clostridium botulinum, cyanobacteria, Gambierdiscus) • Prions • Gene-edited/modified novel microbial agents
Organic Neurotoxins	• Bungarotoxins • Conotoxins • Dendrotoxins • Maculotoxins • Naja toxins • Saxitoxin
Neurotechnological Devices	• Directed energy delivery systems • Transcranial neuromodulatory systems • Neuro-nanomaterial agents

Sources: James Giordano and Rachel Wurzman, "Neurotechnologies as Weapons in National Intelligence and Defense—An Overview," *Synesis: A Journal of Science, Technology, Ethics, and Policy* 2, no. 1 (2011): T55-T71; Rachel Wurzman and James Giordano, "NEURINT and Neuroweapons: Neurotechnologies in National Intelligence and Defense," in *Neurotechnology in National Security and Defense* (Boca Raton, FL: CRC Press, 2014), 104–139.

While many types of weaponizable neuroS/T (for example, chemicals, biological agents, and toxins) have been addressed in and by extant forums, treaties, conventions, and laws, other newer techniques and technologies have not.[4] Thus, particular advances in neuroS/T have an increased potential for dual use and direct use in WINS. In this light, this article (1) presents the WINS utility and possible applicability of gene editing methods, nanoparticles, and other tools that can modify the central nervous system; (2) discusses the value and vulnerabilities of big data and bio-cybersecurity in WINS; (3) posits how such developments bring into stark relief existing gaps in international biological and chemical weapons conventions; and (4) proposes steps toward rectification of current and future oversight and governance.

Dual and Direct WINS Use Radical Leveling and Emerging NeuroS/T

Advancements in human genome sequencing, gene editing technologies, and other ancillary sciences (such as nanotechnology) have been instrumental to improving understanding and targeting of genetic mechanisms involved in several organisms' structures and functions. In 1990, the United States initiated the Human Genome Project. By 2004, a draft had been completed of a significant sequence of the human genome.[5] This knowledge was paired with the use of genome-wide association studies that can determine if any variation or mutation is associated with specific traits (for example, a disease or physiological function).[6] Taken together with other genetic and genomic approaches, such emerging methods and tools have afforded the ability to identify and affect genes that are associated with or contribute to structure, functions, and abnormalities of the nervous system (that is, neurogenetics). This progress in neurogenetics has led to growing consideration of such assessments and modifications for use in WINS applications.[7]

Emerging Techniques Important for Neurogenetics

Gene editing (directly modifying an organism's genetic material to achieve a desired effect and outcome) has been used for several decades. It has been intended and employed for treating a variety of conditions, including immunodeficiency and blood disorders and types of cancers. Gene editing methods were augmented by the discovery of certain nucleases (for example, zinc finger nuclease).[8] However, despite some successes, difficulties with its design and application led to the development and use of simpler methods, most notably, clustered regularly interspaced short palindromic repeats (CRISPR) and the associated Cas9 nuclease.[9] Such new, emerging, and relatively easy to obtain and use gene editing tools could be influential to the creation of novel neuroweapons.[10] Of course, like any method, the uses of CRISPR/Cas systems have limitations. Yet these may not necessarily hinder their utility. In fact, such issues appear to be little more than proverbial "speed bumps" on the path to broadening capabilities afforded by CRISPR and related techniques.

It had been thought that the clinical use of CRISPR-type techniques represented a future possibility. However, a recent report on the administration of CRISPR-modified cells to human embryos in China (to generate an inherited resistance to HIV, smallpox, and cholera) has created a new timetable—and need for current guidelines—for human gene editing.[11] To wit, in March 2019, the World Health Organization's newly formed advisory committee for international governance on human genome editing declared such modifications to human germlines to be "irresponsible."[12] The committee proposed the need for a central registry of human genome editing research in order to facilitate more detailed insight to—and stringent oversight of—risks and hazards.

We agree with and support these actions. It is likely that the ability to modify existing microbes

Cut of replacing part of a DNA molecule

and other organisms will permit "side-stepping" the current Biological and Toxin Weapons Convention (BTWC) in the production of new bioweapons, and thus may necessitate revision of how such treaties categorize and identify agents that can pose risk and threats to global health and security.[13] The recognition and acknowledgment that CRISPR methods could be used to generate novel biological weapons have also prompted studies of reversing CRISPR-induced effects. A recent article in the *MIT Technology Review* identified laboratories that are working to find "anti-CRISPR" molecules: proteins in nature that can "turn off" CRISPR-induced gene edits.[14] Such endeavors reflect steps to control open source research and deter the use of gene editing to produce biological weapons or agents that otherwise negatively affect global health.

While these mitigative and preventive efforts are laudable, it should be noted that such regulation and attempts at restriction may not be encompassing or sufficient. In June 2019, a Russian scientist declared plans to implant gene-edited embryos into women.[15] Clearly, this announcement came after the aforementioned appeals for international constraint of germline editing, thereby reinforcing the reality that CRISPR-based methods are relatively easy to develop and use but not necessarily easy to govern, monitor, and/or control.[16] Of growing concern in this light are clandestine enterprises (biohacking) and research activities of nation-states, virtual nations, and/or nonstate actors that blatantly disregard international standards and guidelines.

Nanomaterials, NeuroS/T, and Bioweapons

Nanotechnology has been shown to be useful in controlling, guiding, and delivering molecules in biological systems to produce desired effects, and this has improved brain imaging and neuroactive drug delivery.[17] As well, targeting molecules using nanotechnology has increased the possibility of

genetically editing the brain.[18] For example, nanolipoproteins (NLPs) mimic naturally occurring molecules and can be used to carry various biological substances (for example, nucleic acids, proteins, and other small compounds) to a desired location in the brain.[19] Because these NLPs closely mimic molecules occurring naturally in humans, detecting their use (for example, in novel neuroweapons) would be difficult.[20] Some proof of concept can be drawn from a 2019 study that used a mouse model to demonstrate the use of such nanotechnological stabilizing methods, the ability to transport modified molecules to the brain (that would otherwise not be possible), and to target and alter specific neural genes in the adult brain.[21] Such methods could be used to genetically enhance neural structures and functions of their own personnel, as well as design novel agents that could degrade adversarial targets. Other applications of nanotechnology are enabling:

- insertion of very small-scale (nano) devices to remotely control organs and/or organisms
- modification of existing and/or creation of new neuropathogens (for example, nanoparticulate matter capable of exerting pathogenic effects in living organisms)
- enhanced delivery methods of drugs and/or toxins
- the disguise of organic molecules to avoid their detection.[22]

Nanotechnology is considered a relatively new science, and it remains unchecked by international treaties despite its viability and utility for various WINS applications.

Modified, non-infectious viruses have also been used as scaffolding to transport materials to edit genetic material.[23] The lentiviruses (immunodeficiency viruses) have been favored because of their ability to integrate their genetic material (including any desired gene edits) to chromosomes of a variety of human cell types.[24] This form of gene editing was used in a recent experiment that employed a modified Simian immunodeficiency virus to introduce the human *MCPH1* gene (a major genetic factor in human brain evolution) into a non-human primate (a rhesus monkey).[25] Following successful lentivirus-facilitated *MCPH1* gene delivery, the monkeys showed decreased reaction times and enhanced short-term memory. Modifying the genome of non-human primates to make them more similar to humans may yield novel models for neurogenetic research and may speed the pace of translational research for human applications. However, we believe that it is important to question what types of neurogenetic research (for example, development of optimized functions and traits, modification of brain maturation or aging, resistance or susceptibility to particular pathogens) and toward what ends research findings, capabilities, and tools will be applied. In this regard, dual and direct WINS uses are not beyond the pale of possibility.[26]

Neurodata on the Molecular Level

Advances in both neurogenetic research and its applications are critically reliant on leveraging biological "big data" ("biodata"). Indeed, the digitization of biology is beginning to transform all of the life sciences, and automation of lab and medical procedures will manage and perform most tasks. The "digitization of biology" refers to the literal translation of the nucleotide codes of DNA to the binary structure (ones and zeros) of computer code. DNA sequences can now be databased and mined and, in these ways, enable computerized experimentation and/or design. Fully extrapolating information in digital contexts to meaningful biological study or the production of engineered organisms has additional dimensions and nuances. This leap from nucleotide data sequences recorded in databases, to forms and functions viable for biological predictions and product syntheses is known as *abstraction*.[27] Valuable abstraction requires extensive genomic

data analysis, using a complex set of computational tools, algorithms, and bioinformatics programs. If and when it is well articulated, the near future use of such high-quality abstraction could enable biological engineers to simply type in desired features for a biological protein/enzyme, or even an entire microbe, and receive those designs as outputs. In fact, such "computer-generated output" would not even require the engineer to have direct knowledge of the genetic sequences involved.

Still, the more complex the organism, the greater the computing and data storage power necessary. For example, one might readily be able to use open source software to engineer a soil microbe, but engineering human DNA in such ways might demand considerably more computational time on high-performance processors—at least at present. These challenges have fostered a host of international research enterprises aimed at opportunizing access to the human genome and iterative computational capability in ways that allow for rapid acquisition and translation of biodata to products, methods, and outcomes.

The U.S. National Center for Biotechnology Information website was created in 1998, and it remains one of the largest resources for biological information, being continuously updated by the U.S. National Institutes of Health, the DNA Data Bank of Japan, and the European Nucleotide Archive.[28] This has prompted other agencies'/companies' own efforts at DNA sequencing, and has enabled human and other genomes to be readily available (with other databases and/or tools) with unrestricted access (see Table 2). Recent attention has been focused on creating means of predicting and inhibiting the persistent problem of off-target mutations of gene editing (as seen for example, in the Chinese "CRISPR babies").[29] Computational algorithms have proven to be relatively affordable, quick, and useful means of assessing any potential off-target effects. Programs such as CRISPOR, CHOPCHOP, CRISPResso, Cas-Offinder, and Off-Spotter allow more accurate guidance of RNA design, acquisition, use of protospacer adjacent motif data, and facile adaptation of genetic modification techniques for use in desired organisms.[30] Computational programs can be augmented by both in vitro genome analysis tools (such as CIRCLE-seq, SITE-seq, and others) and in vivo methods (VIVO, BLISS, etc.), which afford precision identification of both on- and off-target sites in specific cell types in an organism.[31]

Automation

Iterative automation is changing much of how bioscientific research is implemented. Machine systems are now able to execute a number of tasks that are routinely performed by humans, and in this way, machine systems can control many physical aspects of biological platforms and/or human-machine interfaces. For example, recent publications have described working robotic automation systems that reduce the time it takes to conduct synthetic biology experiments.[32] Of note, a "digital-to-biological converter" has been described that can use digital DNA sequence information and produce DNA templates, RNA molecules, proteins, and viral particles.[33] Furthermore, automated devices that monitor and/or control biological processes produce abundant data that can be shared and stored through cloud computing networks. As noted, the acquisition, use, and abstraction of such data require advanced computational software, algorithms, and bioinformatics. These processes also can be automated and have already proven to improve biological laboratory efficiency, and thus are beginning to be used more widely.[34]

As digitization and automation become more available, continue to advance, and are further integrated into various laboratories and medical centers, the procurement of and access to biodata will greatly simplify several dimensions and domains of biomedical research. Many countries have overtly—or

more surreptitiously—begun to collect and utilize data to foster biotechnological innovation.[35] Of particular note are efforts by China to collect vast quantities of genetic data in an initiative to construct a working database of its citizens.[36] When fully operational, facilities in the city of Nanjing will sequence 400,000 to 500,000 samples per year and will be able to track individuals to obtain environmental and behavioral data.[37] China's cultural and political needs, values, and philosophies may establish ethico-legal parameters that allow extensive acquisition, access, and use of biological (and psycho-social) data in ways that are not viable in other countries. The concurrent collection of genetic and environmental/behavioral data can be essential to acquiring considerable knowledge about diverse aspects of human terrain.[38] Per the adage that knowledge is power, this may expedite discovery and development of novel forms and capabilities of neuroS/T that can be employed to leverage strategically latent political effects worldwide.

With more laboratories and medical centers incorporating automation into their current systems, it is probable that a number of challenges and problems will be encountered and/or incurred.[39] For instance, whole human genomic data (for example, as collected by companies like *23andMe*, or *Ancestry*) are instrumental to creating and establishing a broader knowledge base (and palette of accessible information) about genes, inheritance,

Table 2. Public Databases Used for Retrieving Biological Information

Databases	Foci, Function(s)
NCBI Entrez System	Diverse, integrated set of databases focusing on six core areas • Literature: medical and scientific abstracts, full-text articles, books, and reports • Genes: sequences and annotations used as references for studies of orthologs structure, expression, and evolution • Genetics: heritable DNA variations, associations with human pathologies, and clinical diagnostics and treatments • Proteins: 3-D structures, protein sequences, and tools for studies of functional protein domains and active sites • Genomes: sequence assemblies, large-scale functional genomic data, and source biological samples • Chemicals: repository of chemical information, molecular pathways, and tools for bioactivity screening Source: https://www.ncbi.nlm.nih.gov/search/
GeneCards: The Human Gene Database	Searchable, integrative database providing comprehensive, user-friendly information on all annotated and predicted human genes Source: https://www.genecards.org/
U.S. Department of Energy Joint Genome Institute	Provides integrated high-throughput sequencing, DNA design and synthesis, metabolomics, and computational analysis that enable systems-based scientific approaches to these tasks Source: https://jgi.doe.gov/about-us/
NASA GeneLab Data System	Provides access to experiments undertaken aboard the International Space Station that explore the molecular responses of terrestrial biology to spaceflight environments Source: https://genelab-data.ndc.nasa.gov/genelab/

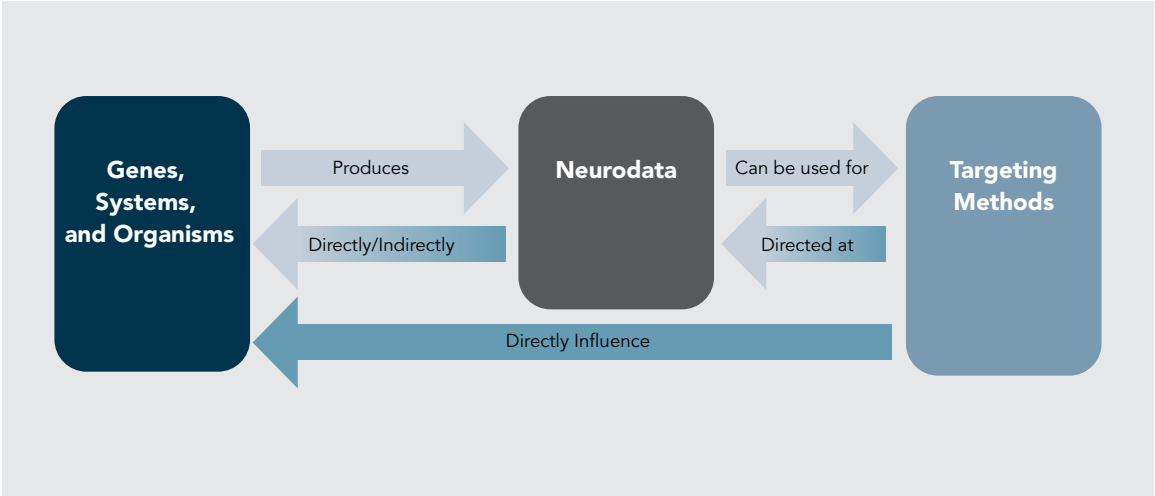
and dimensions of human intelligence, emotion, and actions. Recently described as "sociogenomics," there is, of course, the possibility that this information (about an individual's genotypic predilection for neurological disease, phenotypes, and/or behaviors) could be used to discriminate against or extort targeted individuals and/or groups.[40] As well, the acquisition and use of such data could enable exploitation of particular genetic vulnerabilities to incur harm. Health records, health insurance profiles, or other clinical databases in which such information is housed have become vulnerable to direct cyberattacks on IT infrastructures.[41]

Risks of Neurodata

The intersecting vulnerabilities of computational systems and biological information are focal to the scope and activities of the emerging field of "cyberbiosecurity." Jean Peccoud and colleagues define this discipline to entail (1) "understanding vulnerabilites to unwanted surveillance, intrusions, and . . . harmful activities which can occur at the interfaces of . . . medical sciences, cyber, cyber-physical . . . and infrastructure systems" and (2) "measures to prevent, protect, mitigate, investigate, and attribute such risks as it pertains to security, competitiveness, and resilience."[42] Previously we have analyzed the unique risks associated with biodata along a continuum of harms from individual privacy, to physical harm to individuals and groups—and we have highlighted the cyberbiosecurity risks specific to these domains.[43] Here, we direct a similar examination by identifying the subset of biodata obtained from and operationalized within neuroS/T. We believe this subset represents a specialized landscape of vulnerabilities unlike any other in the cyberbiosecurity arena, as it could impact human mental health, cognitive states, emotional states, decisionmaking, and behavior. Such ability to coerce or otherwise control human beings via access to neurobiological manipulation is profound in both WINS and sociopolitical contexts. We envision two possible vectors of threat/harm: (1) the manipulation of neurodata in order to incur a direct/indirect effect on the way an individual or group is regarded and/or treated; and (2) the access and use of neurodata to design a precision effect on an individual or a group (see Figure 1).

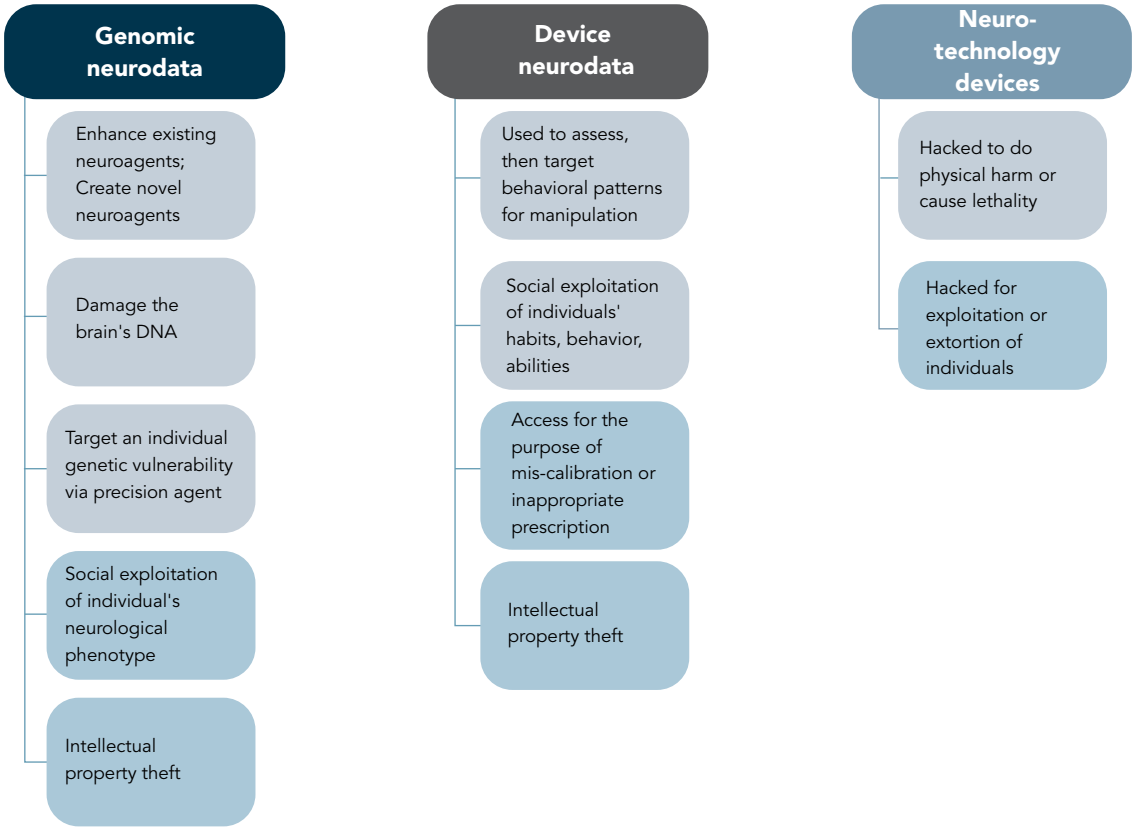
Technological advances are expanding the type and variety of tools that can afford human-machine interfacing (HMI) for maintaining or improving

Figure 1. Using Neurodata for WINS Operations



Source: Author provided.

Figure 2. Risks



Source: Author provided.

health, and/or modifying (optimizing or negatively affecting) human neurocognitive and behavioral capabilities and performance.[44] A timely example of this type of HMI is the *Neuralink* system proposed by Elon Musk as a minimally invasive intervention that could modulate selective brain networks and functions.[45] The iterative development and utility of these devices are critically dependent upon the acquisition and use of diverse types and levels of data. These data, while force-multiplying the capabilities of neuroS/T, also render distinct risks in their relative susceptibility to hacking and manipulation.[46] While tampering of any HMI is a cyberbiosecurity vulnerability, the capacity to access and control aspects of human cognition, emotion, and behavior incurs a special category of risk (see Figure 2). In these cases, cyberbiosecurity solutions will entail protection afforded to neurotechnological devices, and whether and how the information cued on such devices is accessed and shared by others.

We consider these potential dual uses of neurodata to be a first but significant step in a pathway intended to produce neuropsychiatric threat and harm. Current treaties and conventions (for example, the Biological and Toxin Weapons Convention [BTWC] and Chemical Weapons Convention [CWC]) do not (yet) recognize, address, and hence govern the weaponized use of neurodata (or other biodata) and/or neuro-genetic modifiers.[47] Thus, we believe and posit that it is important to acknowledge

the role of—and need to protect and regulate—neurodata. Determination of who has access to these data and how access is provided should be considered and incorporated as fundamental components of any meaningful cyberbiosecurity solution on a relatively local scale. More broadly, such protections should be elements of future policy and governance in this realm.

Toward Regulations and Security

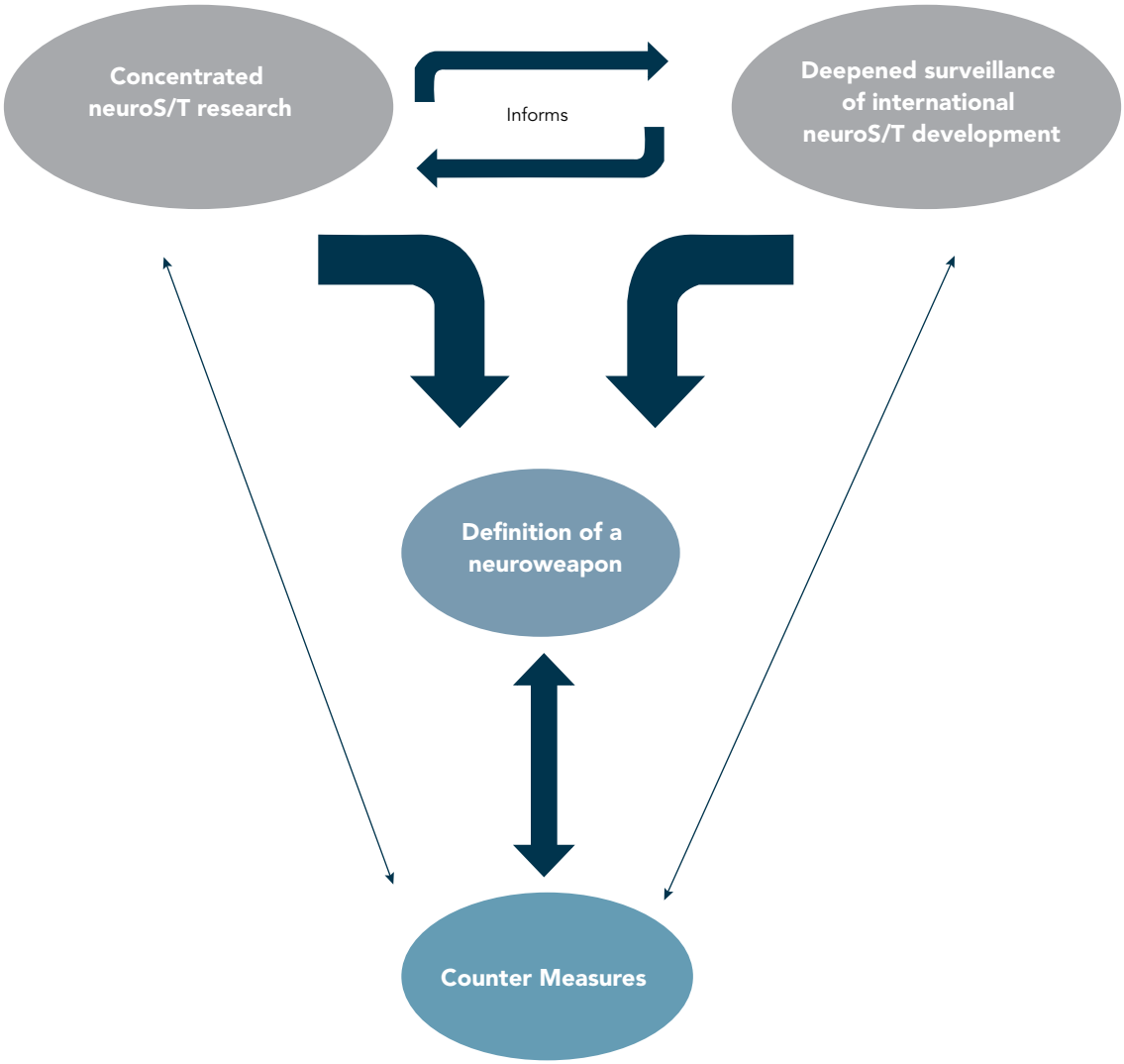
Regardless of current limitations, we believe that the BTWC and CWC can continue to be important mechanisms for international weapons control. The development, production, acquisition, retention, and/or stockpiling of defined neuro-microbiologicals, select chemicals, and toxins are prohibited by these two conventions. Yet these treaties are generally reactive and address biological and chemical weapons that have been used in the past. As well, the BTWC and CWC definitions of weapons were purposively intended to be vague in order to avoid constricted classification. This reactivity and system of classification do not account for (1) use of neurocognitive science (for example, neuropharmacological or neurotechnological augmentation) to optimize and enhance human performance in WINS operations; (2) development of novel pathogens via emerging technologies (for example, gene editing, nanoengineering, etc.); (3) the potential effect of ancillary techniques and technologies on existing biochemical agents; (4) specific neurotechnological devices that can be employed as weapons; and (5) the possibility of the human actor as a "biological agent."[48] Recent advancements and continued convergence of the brain sciences, genetics, neurotechnologies, and neurodata make the aforementioned possibilities rapidly realizable and urgent to consider and address.

Such risks and threats are greater as neuroscience becomes a more international enterprise and as nonstate actors and unregulated states acquire neuroS/T capabilities that can be used to achieve new balances of power. At their core, the viability and effectiveness of the BTWC and CWC are reliant on participatory states' signature/ratification and acting in good faith. Without this standard, such agreements are relatively meaningless. Yet, the United Nations (UN) does not have statutes that make it mandatory to sign or ratify these conventions. Although UN Security Council Resolution 1540 (adopted in 2004) intended to target nonstate actors' production and acquisition of weapons of mass destruction, it requires UN countries to modify their own legislation to exercise such controls. Enforcing the resolution is therefore dependent upon UN states' proactive engagement and effectiveness, and thus fails to provide broad-based oversight and governance.[49]

Without proper surveillance and international cooperation, there is opportunity to bypass the BTWC, CWC, and other international regulations through (1) various types of commercial veiling strategies; (2) venture capitalist financing of "do-it-yourself"/biohacker scientists to conduct neuroS/T research for malevolent purposes; (3) research tourism that attracts scientists to undertake neuroS/T research and development in countries with capricious (or nefarious) agendas; (4) medical tourism, which encourages ethically problematic clinical practices; (5) defining a country's research and use of weaponizable neuroS/T as "defensive" or for "intelligence" purposes; and (6) exploiting export codes of "dual-use" materials and technologies. Given these possibilities, we believe that it is increasingly important to analyze, quantify, and predict how the brain sciences can—and likely will—be developed and employed by foreign competitors and adversaries in both non-kinetic and kinetic ways.

The current pace and scope of global neuroS/T research and development are indicative that this problem will only increase in years to

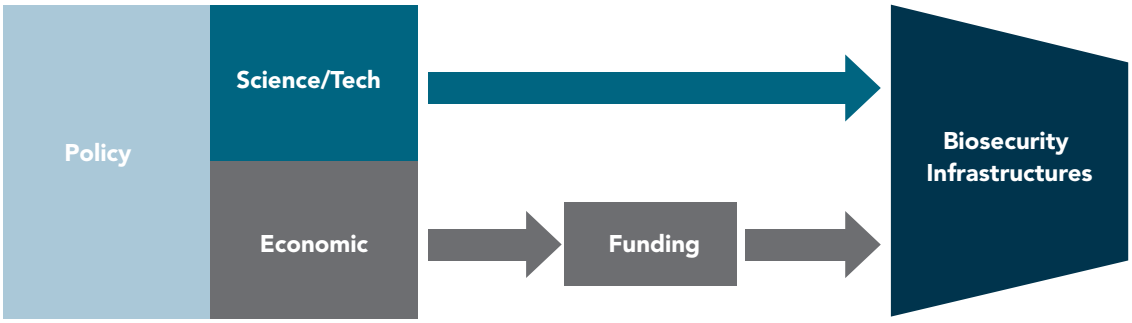
Figure 3. Defining and Regulating Neuroweapons through Research and Surveillance



Source: Author provided.

come.[50] The United States and its allies must acknowledge the risks that the brain sciences and ancillary technologies pose for potential applications in dual or direct uses for WINS purposes, and these developments and risks must be fully evaluated in order to establish and implement effective preparedness and countermeasures (see Figure 3). We see this as a multi-step process. First, the United States must engage extensive and focused research to better understand the current and near-term weaponization of neuroS/T. Several countries already have dual-use initiatives and/or military programs dedicated to neuroS/T, and not all are amenable or accessible to international surveillance and inspection.[51] We opine that at present, there is a significant gap in the ability to forecast state-sponsored research and how nonstate actors could and will be able to harness

Figure 4. Structure and Dynamics of Support for Effective Biosecurity Programs in the 21st Century



Source: Author provided.

extant neuroS/T for WINS applications.

To this point, we call for deeper and more granular surveillance of international neuroS/T research and use agendas. The European Union (EU) Dual-Use Coordination Group states that while approximately 20 percent of EU exports are "dual-use" goods, only 2.4 percent of those require export-license (the United States requires only 1 percent of "dual-use" goods to be authorized). A joint statement by the European Parliament, Council of the European Union, and the European Commission's Dual-Use Regulation calls for "a high level of security and adequate transparency without impeding competitiveness and legitimate trade in dual-use items."[52] Toward these ends, assessing the scientific literature is an important step, as it could depict present and future research trends and afford means to monitor researchers who are knowledgeable, skilled, and able to exercise methods of creating neuroweapons. However, to appreciate the full scope of weaponizable neuroS/T, surveillance should focus on (1) activities of university and research sites; (2) the extent and directions of private and public support of research and development; (3) efforts toward recruitment of researchers; (4) neuroS/T commercialization; (5) current/future military postures; and (6) current/future neuroS/T markets and the potential for leveraging developments in this field for economic profit and global power.

International surveillance and research examining the ways that neuroS/T is being employed in WINS initiatives must be mutually supportive. Such reciprocity will be important to more accurately and efficiently (1) define which neuroS/T could have potential non-kinetic and/or kinetic capabilities; (2) understand present and future trends in research and development; and (3) identify specific research centers and personnel capable of—and involved in—creating neuroweapons (see Figure 3). We assert that the effective function of any competent, capable, and valuable biosecurity program requires two non–mutually exclusive factors. First is dedication to and flexibility in developing ongoing and revisable methods of identification, definition, classification, and regulation of current and emerging neuroweapons; and second is political support and sustained funding.

As shown in Figure 4, sound policies are important to the establishment, structure, and sustained functions of a biosecurity enterprise. Funding is essential to creating, maintaining, and expanding the resources, personnel, and activities of biosecurity infrastructures. However, policy is the means by which any funding is identified, appropriated, and allocated. Thus, ongoing efforts of surveillance, evaluation, and preparedness of science and technology mandate engagement and provisions of effort(s) to inform policy development and enforcement. PRISM

Acknowledgments

James Giordano's work is supported in part by the Henry M. Jackson Foundation for the Advancement of Military Medicine; Leadership Initiatives; and federal funds UL1TR001409 from the National Center for Advancing Translational Sciences, National Institutes of Health, through the Clinical and Translational Science Awards Program, a trademark of the Department of Health and Human Services, part of the Roadmap Initiative, "Re-Engineering the Clinical Research Enterprise." Diane DiEuliis acknowledges research support of the Center for the Study of Weapons of Mass Destruction, National Defense University. PRISM

Notes

[1] Patricia DeGennaro, "The Gray Zone and Intelligence Preparation of the Battle Space," *Small Wars Journal Mad Scientist* no. 13 (2016).

[2] Jonathan D. Moreno, Michael Tennison, and James Giordano, "Security Threats Versus Aggregated Truths: Ethical Issues in the Use of Neuroscience and Neurotechnology for National Security," in *Neuroethics: Anticipating the Future*, ed. Judy Illes (New York: Oxford University Press, 2017).

[3] Joseph DeFranco et al., "Emerging Technologies for Disruptive Effects in Non-Kinetic Engagements," *Journal of the Homeland Defense & Security Information Analysis Center* 6, no. 2 (2019): 48–55.

[4] Malcolm Dando, "Neuroscience Advances and Future Warfare," *Handbook of Neuroethics* (2015): 1785–1800.

[5] J. Craig Venter et al., "The Sequence of the Human Genome," *Science* 291, no. 5507 (2001): 1304–1351; International Human Genome Sequencing Consortium, "Finishing the Euchromatic Sequence of the Human Genome," *Nature* 431, no. 7011 (2004): 931.

[6] Angeliki Vgontzas and William Renthal, "Introduction to Neurogenetics," *American Journal of Medicine* 132, no. 2 (2019): 142–152; Alkes L. Price et al., "Principal Components Analysis Corrects for Stratification in Genome-wide Association Studies," *Nature Genetics* 38, no. 8 (2006): 904; Iris E. Jansen et al., "Genome-wide Meta-analysis Identifies New Loci and Functional Pathways Influencing Alzheimer's Disease Risk," 2019; Andreas Papassotiropoulos and J-F. Dominique, "Genetics of Human Episodic Memory: Dealing with Complexity," *Trends in Cognitive Sciences* 15, no. 9 (2011): 381–387.

[7] Diane DiEuliis and James Giordano, "Gene Editing Using CRISPR/Cas9: Implications for Dual-use and Biosecurity," *Protein & Cell* 9, no. 3 (2018): 239–240; Huda Y. Zoghbi and Stephen T. Warren, "Neurogenetics: Advancing the 'Next Generation' of Brain Research," *Neuron* 68, no. 2 (2010): 165–173.

[8] Yang-Gyun Kim, Jooyeun Cha, and Srinivasan Chandrasegaran, "Hybrid Restriction Enzymes: Zinc Finger Fusions to Fok I Cleavage Domain," *Proceedings of the National Academy of Sciences* 93, no. 3 (1996): 1156–1160.

[9] Dana Carroll, "Genome Engineering with Zinc-Finger Nucleases," *Genetics* 188, no. 4 (2011): 773–782; Elena E. Perez et al., "Establishment of HIV-1 Resistance in CD4+ T cells by Genome Editing Using Zinc-Finger Nucleases," *Nature Biotechnology* 26, no. 7 (2008): 808; A.A. Nemudryi et al., "TALEN and CRISPR/Cas Genome Editing Systems: Tools of Discovery," *Acta Naturae* 6, no. 3 (2014): 22.

[10] Diane DiEuliis and James Giordano, "Why Gene Editors Like CRISPR/Cas May Be A Game-Changer for Neuroweapons," *Health Security* 15, no. 3 (2017): 296–302.

[11] Antonio Regalado, "Chinese Scientists Are Creating CRISPR Babies," *MIT Technology Review*, November 25, 2018, available at <https://www.technologyreview.com/s/612458/exclusive-chinese-scientists-are-creating-crispr-babies/>; David Cyranoski, "CRISPR Gene-Editing Tested in a Person for the First Time," *Nature News* 539, no. 7630 (2016): 479.

[12] World Health Organization, "WHO Expert Panel Paves Way for Strong International Governance on Human Genome Editing," March 19, 2019, available at <https://www.who.int/news-room/detail/19-03-2019-who-expert-panel-paves-way-for-strong-international-governance-on-human-genome-editing>.

[13] Daniel Gerstein and James Giordano, "Rethinking the Biological and Toxin Weapons Convention?" *Health Security* 15, no. 6 (2017): 638–641.

[14] Antonio Regalado, "The Search for the Kryptonite that Can Stop CRISPR," *MIT Technology Review*, May 2, 2019, available at <https://www.technologyreview.com/s/613309/the-search-for-the-kryptonite-that-can-stop-crispr/>.

[15] D. Cyranoski, "Russian Biologist Plans More CRISPR-edited Babies," *Nature* 570, no. 7760 (2019): 145.

[16] C.D. Wolinetz and F.S. Collins, "NIH Supports Call for Moratorium on Clinical Uses of Germline Gene Editing," (2019): 175.

[17] Florence Sanchez and Konstantin Sobolev, "Nanotechnology in Concrete—A Review," *Construction and Building Materials* 24, no. 11 (2010): 2060–2071; Andrea Gropman, "Applying Advances in Neurogenetics to Medical Practice," 2006: 677–685.

[18] DeFranco et al., "Emerging Technologies."

[19] Nicholas O. Fischer et al., "Evaluation Of Nanolipoprotein Particles (NLPs) as an In Vivo Delivery Platform," *PloS One* 9, no. 3 (2014): e93342.

[20] National Academies of Sciences, Engineering, and Medicine, *Biodefense in the Age of Synthetic Biology* (Washington, DC: National Academies Press, 2018).

[21] Sumiyo Watanabe et al., "In Vivo Rendezvous of Small Nucleic Acid Drugs with Charge-matched Block Catiomers to Target Cancers," *Nature Communications* 10, no. 1 (2019): 1894.

[22] DeFranco et al., "Emerging Technologies."

[23] Ina Balke and Andris Zeltins, "Use of Plant Viruses and Virus-Like Particles for the Creation of Novel Vaccines," *Advanced Drug Delivery Reviews* (2018).

[24] Michael C. Milone and Una O'Doherty, "Clinical use of Lentiviral Vectors," *Leukemia* 32, no. 7 (2018): 1529.

[25] Lei Shi et al., "Transgenic Rhesus Monkeys Carrying the Human MCPH1 Gene Copies Show Human-like Neoteny of Brain Development," *National Science Review* 6, no. 3 (2019): 480–493.

[26] Guillermo Palchik, Celeste Chen, and James Giordano, "Monkey Business? Development, Influence, and Ethics of Potentially Dual-use Brain Science on the World Stage," *Neuroethics* 11, no. 1 (2018): 111–114.

[27] Christopher Ochs et al., "Quality Assurance of the Gene Ontology Using Abstraction Networks," *Journal of Bioinformatics and Computational Biology* 14, no. 3 (2016): 1642001.

[28] David L. Wheeler et al., "Database Resources of the National Center for Biotechnology Information," *Nucleic Acids Research* 35, no. suppl. 1 (2006): D5-D12.

[29] Joseph DeFranco and James Giordano, "Designer Genes: Made in China?" Mad Scientist Laboratory, post no. 66, August 1, 2019, available at <https://madsciblog.tradoc.army.mil/166-designer-genes-made-in-china/>.

[30] For more information on in silico genome analysis tools, see Maximilian Haeussler et al., "Evaluation of Off-target and On-target Scoring Algorithms and Integration into the Guide RNA Selection Tool CRISPOR," *Genome Biology* 17, no. 1 (2016): 148; Tessa G. Montague et al., "CHOPCHOP: A CRISPR/Cas9 and TALEN Web Tool for Genome Editing," *Nucleic Acids Research* 42, no. W1 (2014): W401–W407; Luca Pinello et al., "Analyzing CRISPR Genome-Editing Experiments with Crispresso," *Nature Biotechnology* 34, no. 7 (2016): 695; Sangsu Bae, Jeongbin Park, and Jin-Soo Kim, "Cas-OFFinder: A Fast and Versatile Algorithm that Searches for Potential Off-target Sites of Cas9 RNA-guided Endonucleases," *Bioinformatics* 30, no. 10 (2014): 1473–1475; and Venetia Pliatsika and Isidore Rigoutsos "'Off-Spotter': Very Fast and Exhaustive Enumeration of Genomic Lookalikes for Designing CRISPR/Cas Guide RNAs," *Biology Direct* 10, no. 1 (2015): 4.

[31] For more information on in vitro genome analysis tools, see Shengdar Q. Tsai et al., "CIRCLE-seq: A Highly Sensitive In Vitro Screen for Genome-wide CRISPR–Cas9 Nuclease Off-targets," *Nature Methods* 14, no. 6 (2017): 607; and Peter Cameron et al., "Mapping the Genomic Landscape of CRISPR–Cas9 Cleavage," *Nature Methods* 14, no. 6 (2017): 600. For more information on in vivo genome analysis tools, see Pinar Akcakaya et al., "In Vivo CRISPR Editing with No Detectable Genome-wide Off-target Mutations," *Nature* 561, no. 7723 (2018): 416; and Winston X. Yan et al., "BLISS Is a Versatile and Quantitative Method for Genome-wide Profiling of DNA Double-strand Breaks," *Nature Communications* 8 (2017): 15058.

[32] Blake Marshal Elias, "High Throughput Pin-tool Based Automated DNA Assembly," PhD diss., Massachusetts Institute of Technology, 2018; Michael I. Sadowski, Chris Grant, and Tim S. Fell, "Harnessing QbD, Programming Languages, and Automation for Reproducible Biology," Trends in Biotechnology 34, no. 3 (2016): 214–227.

[33] Kent S. Boles et al., "Digital-to-Biological Converter for On-demand Production of Biologics," *Nature Biotechnology* 35, no. 7 (2017): 672.

[34] Anthony Croxatto et al., "Laboratory Automation in Clinical Bacteriology: What System to Choose?" *Clinical Microbiology and Infection* 2, no. 3 (2016): 217–235; Jacob Nichols et al., "2069. Automation Process Improving Microbiological Laboratory Efficiency," *Open Forum Infectious Diseases* 5, suppl. 1 (New York: Oxford University Press, 2018), S604.

[35] For example, Hannah Denham and Drew Harwell,

"Panic over Russian Company's FaceApp Is a Sign of New Distrust of the Internet," *Washington Post*, July 18, 2019, available at <https://www.washingtonpost.com/technology/2019/07/18/heres-what-we-know-about-russian-company-behind-faceapp/>.

[36] Claudia Geib, "A Chinese Province is Sequencing One Million of Its Residents' Genomes," *Futurism*, November 8, 2017, available at <https://futurism.com/chinese-province-sequencing-1-million-residents-genomes>.

[37] Nanjing YiGenCloud, "Nanjing YiGenCloud Institute Aims to Speed Up the Process of China's Precision Medicine with 'Intelligence,'" Cison PR Newswire, May 27, 2019, available at <https://www.prnewswire.com/news-releases/nanjing-yigencloud-institute-aims-to-speed-up-the-process-of-chinas-precision-medicine-with-intelligence-300856584.html>.

[38] This refers to the field of neuroepigenetics, which is outside the purview of this paper. For more information, see J. David Sweatt, "The Emerging Field of Neuroepigenetics," *Neuron* 80, no. 3 (2013): 624–632.

[39] Claudia Archetti et al., "Clinical Laboratory Automation: A Case Study," *Journal of Public Health Research* 6, no. 1 (2017); Gustavo de Freitas Nobre, Marcelo Kalichsztein, and Marcelo Martínez Ramos, "Hospital Bed Automation System and Methods for Performing Signal Read and Correlation as well as Real-time Data Processing," U.S. Patent Application 16/300,272, filed May 16, 2019.

[40] Nathaniel Comfort, "Sociogenomics Is Opening a New Door to Eugenics," *MIT Technology Review*, October 23, 2018, available at <https://www.technologyreview.com/s/612275/sociogenomics-is-opening-a-new-door-to-eugenics/>.

[41] Lukasz Piwek et al., "The Rise of Consumer Health Wearables: Promises and Barriers," *PLoS Medicine* 13, no. 2 (2016): e1001953.

[42] Jean Peccoud et al., "Cyberbiosecurity: From Naive Trust to Risk Awareness," *Trends in Biotechnology* 36, no. 1 (2018): 4–7.

[43] Diane DiEuliis, Chuck D. Lutes, and James Giordano, "Biodata Risks and Synthetic Biology: A Critical Juncture," *Journal of Bioterror and Biodefense* 9, no. 159 (2018): 2.

[44] Raza Qazi et al., "Wireless Optofluidic Brain Probes for Chronic Neuropharmacology and Photostimulation," *Nature Biomedical Engineering* (2019): 1–15.

[45] Joseph DeFranco and James Giordano, "Linking Brains to Machines, and Use of Neurotechnology to the Cultural and Ethical Perspectives of the Current Global Stage," Mad Scientist Laboratory, post no. 168, August 8, 2019, available at <https://madsciblog.tradoc.army.mil/168-linking-brains-to-machines-and-use-of-neurotechnology-to-the-cultural-and-ethical-perspectives-of-the-current-global-stage/>.

[46] Dian DiEuliis and James Giordano, "Neurotechnological Convergence and 'Big Data': A Force-Multiplier Toward Advancing Neuroscience," in *Ethical Reasoning in Big Data*, 71–80, Springer, Cham, 2016.

[47] Malcolm Dando, "Advances in Neuroscience and the Biological and Toxin Weapons Convention," *Biotechnology Research International* (2011); Giordano and Wurzman, "Neurotechnologies as Weapons in National Intelligence and Defense."

[48] Rain Liivoja and Luke Chircop, "Are Enhanced Warfighters Weapons, Means, or Methods of Warfare?" *International Law Studies* 94, no. 1 (2018): 7.

[49] Verification refers to the countries' national regulations and acceptable execution of international legislation. Although countries are forced to implement codes that prevent the existence of agents that do not serve "prophylactic, protective, or other peaceful" purposes, states may choose not to enforce such laws. Enforcement refers to the infliction of retribution to states that do not follow international regulations. Without proper verification of states' adherence to the BTWC, CWC, or UNSCR 1540, it is impossible to enforce a violation by a nation.

[50] Joseph DeFranco, L.R. Bremseth, and James Giordano, "The Importance of Integrative Science/Technology Intelligence (InS/TINT) to the Prediction of Future Vistas of Emerging Threats," Mad Scientist Laboratory, post no. 125, March 13, 2019, available at <https://madsciblog.tradoc.army.mil/125-the-importance-of-integrative-science-technology-intelligence-ins-tint-to-the-prediction-of-future-vistas-of-emerging-threats/>.

[51] Moreno, Tennison, and Giordano, "Security Threats Versus Aggregated Truths."

[52] Christine Aicardi et al., *Dual Use in Neuroscience and Neurotechnology* (London: Human Brain Project Foresight Lab at King's College London, 2017); The European Parliament and the Council of the European Union, "Position (EU) No 5/2014 of the council at First Reading with a view to the adoption of a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items," *Official Journal of the European Communities*, C 100, no. 6 (2014).

The National Security and National Defense Strategies of the United States are built upon a re-emphasis on great power competition.

Strategic Competition for Emerging Military Technologies

Comparative Paths and Patterns

By Michael Raska

One of the most pressing issues in contemporary international relations is the expectation of a new era of intensifying strategic competition, characterized by the confluence of political, economic, and military-technological competitions in the context of major shifts in the global security environment.[1] At the forefront of this growing strategic rivalry is the contest for future supremacy over global security and economic institutional grids between the world's major military powers—the United States, China, and to a lesser degree, Russia.

The Trump Administration has adopted an unprecedentedly combative stance toward China—the 2017 *National Security Strategy* describes China as a "revisionist power . . . that seeks to displace the United States in the Indo–Pacific region," while the 2018 *National Defense Strategy* portrays China as "a strategic competitor" that is using "predatory economics," as well as its growing military capabilities, "to intimidate its neighbors."[2] The shift in U.S. perceptions amounts to a growing realization that its two-part strategy of "engagement and strategic balancing" toward China that began with the Nixon/Kissinger "China opening" in the late 1960s, has failed to achieve its main objective—to integrate China as a "responsible stakeholder" in the existing international system, while preserving a favorable balance of power that would dissuade China from trying to mount a serious challenge in the long-term future.[3] Increasingly, the policy narrative has shifted toward a contrary viewpoint—as a fast–rising power, China "embodies a more enduring strategic challenge"—it is reluctant to accept institutions, border divisions, and hierarchies of political prestige put in place when it was comparatively weak.[4] According to one observer,

> *it would be naïve to assume that China doesn't harbor longer-term strategic ambitions in the region that would allow it to emerge not only as a 'theater peer' of the United States but also as the most formidable Asian power that would be able to contest and effectively deter the United States.*[5]

Strategic competitions between great powers are not new; they have been deeply rooted in history—from the Athenian and Spartan grand strategies during the Peloponnesian War in the fifth century BCE, to the bipolar divide between the Soviet Union and the United States in the Cold War during the second half of the

Dr. Michael Raska is Assistant Professor and Coordinator of the Military Transformations Programme at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore.

20th century. The character of the emerging strategic competition, however, differs from analogies of previous strategic competitions, most recently in the period of the Cold War, when the United States focused solely on maximizing the containment of the Soviet Union across all dimensions—political, economic, ideological, and military—while the Soviet Union countered with comprehensive efforts to shift the overall "correlation of forces" to favor Moscow.[6] Today, the United States faces an array of current and long-term security challenges across different geographical areas, while the Sino–U.S. relationship is much more complex in terms of integrating varying drivers of cooperation, competition, and conflict simultaneously. In other words, the global patterns of the strategic competition in the 21st century are more complex, unpredictable, and diverse, reflecting multiple competitions under different or overlapping sets of rules. Long-term economic interdependencies co-exist with core strategic challenges, while ideological and institutional contests focus on the making and interpretation of rules and norms. Consequently, the ways and means of engaging in strategic competitions vary from pursuing security and prosperity through cooperative and institutional terms strictly in the economic arena, to sharp political-military-technological competition for power and status. The latter essentially embraces the logic of long-term competitive strategies aimed to attain or sustain a comparative advantage—relative to peer adversaries—across geopolitical, technological, military, economic, and other areas in order to significantly constrain competitor's strategic options and choices.[7] At the core of the emerging strategic competition, therefore, is whether China and Russia will have the requisite capabilities to project power in the Indo–Pacific on par with the United States, and how the United States and its key allies in unison with other major powers will respond to such changes.

In this context, this article provides brief contours of the ways and means China, Russia, and the United States attempt to attain or prolong margins of their military-technological superiority in strategic competition for emerging advanced technologies such as artificial intelligence (AI), robotics, additive manufacturing (or 3D printing), and other disruptive technologies. Emerging technologies such as AI are widely regarded to be a crucial element of future military effectiveness and advantage. In theory (and often in practice), the possession of cutting-edge militarily relevant technologies equals more effective weapons systems, which in turn results in greater military power, which in turn translates into greater geopolitical power. For example, the application of novel machine-learning algorithms to diverse problems promises to provide unprecedented capabilities in terms of speed of information processing, automation for weapons platforms and surveillance systems, and ultimately, decision-making for more precision firepower. In doing so, the utility of AI in military affairs seems virtually endless—from real-time analysis of sophisticated cyberattacks and detection of fraudulent imagery to directing autonomous platforms such as drones, to new forms of command and control such as automated battle management systems that analyze big data and provide recommendations for human action. Consequently, the diffusion of AI will have profound implications for how militaries adopt new technologies; how on an operational level, militaries adapt to and apply new technologies, and our understanding of the future battlespace.

However, such technologies and resulting capabilities rarely spread themselves evenly across geopolitical lines. In the case of China, Russia, and the United States, the diffusion of new and potentially powerful militarily relevant technologies—as well as the ability of militaries to exploit potential—varies widely. As with any novel technologies in military affairs, there are complex organizational, conceptual, and operational barriers to innovation. These may include, for example, the reliability of

advanced algorithms to enable systems to learn from surprises and adapt to changes in their environment, to adopting and adapting them into varying force structures and weapons platforms using novel operational concepts, and ultimately, designing ethical codes and safeguards on how to use them. At the same time, "militarily relevant advanced technologies" are becoming harder and harder to identify and classify. Technological advances, especially in the area of military systems, are a continuous, dynamic process; breakthroughs are always occurring, and their impact on military effectiveness and comparative advantage could be both significant and hard to predict at their nascent stages. In particular, many advanced technologies—many of which are embedded in commercial, rather than military industrial sectors—offer new and potentially significant opportunities for defense applications and, in turn, for increasing one's military edge over potential rivals. This can be seen in the convergence of emerging dual-use technologies, conceptualized under the term the "Fourth Industrial Revolution" (4IR) in the following areas (see Figure 1).[8]

The resulting unequal distribution, in turn, naturally affects how these technologies and capabilities may impact regional security and stability. Alliances may become more closely interconnected through technology-sharing and interoperability imperatives, while traditional strategic concepts such as deterrence may be tested through the emergence of different types of conflicts brought by new technologies. Consequently, it is critical to assess the relative abilities of regional militaries to access and leverage new and emerging critical technologies, their likely progress in doing so, and the impediments they may face, ultimately with an eye

Figure 1. Convergence of 4IR Dual-Use Technologies.

Perception, Processing, Cognition	Performance and Materials	Communication, Navigation and Targeting	Manufacturing, Logistics and Supply Chain
• Cloud Computing	• Quantum Computing	• Precision Position, Navigation and Timing	• Robotics
• Big Data Analytics	• Autonomy	• Directed Energy	• Additive Manufacturing
• Artificial Intelligence	• Novel / Smart / BioMaterials	• Electro-Magnetic Weapons	• 4D Printing / Smart Materials
• Cyber capabilities	• Meta-technologies	• Cyber Capabilities	• Synthetic biology manufacturing
• Virtual and Augmented Reality	• Composites for Aerospace	• Unmanned Systems	• Virtual and Augmented Reality Manufacturing / Simulation and Training / Computer Aided Design
• Robotics / Unmanned Systems	• Internet of things	• Hypersonics	
• Advanced Sensors	• Energy capture and storage	• Optical satellite links	
• Internet of things		• Visible light communication	

Source: TX Hammes, "Technologies Converge, Power Diffuses," Paper presented at RSIS-TDSI Seminar '*Disruptive Defence Technologies in Military Operations*', Singapore, June 29, 2016., available at <https://www.rsis.edu.sg/wp-content/uploads/2016/08/ER160823_RSIS-TDSI.pdf>.

toward how it will affect relative gains and losses in regional military capabilities.

Defense Innovation Trajectories: A Comparative Framework

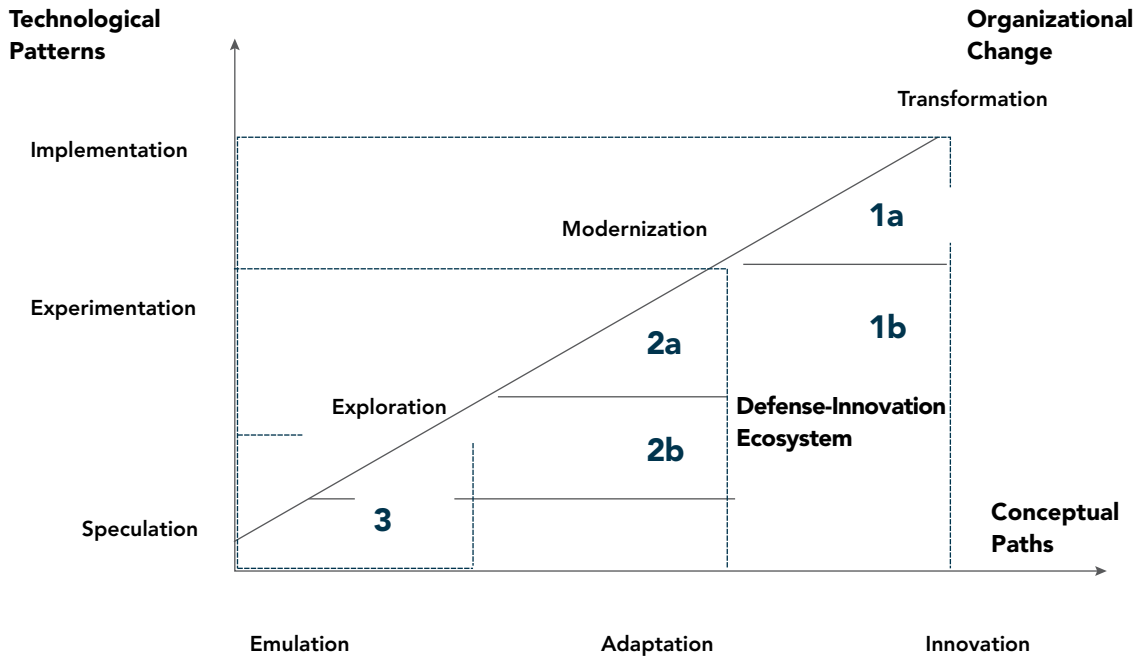
The growing strategic rivalries and the contest for future supremacy between the United States, Russia, and China shape different national responses to the same technological breakthroughs, conditioned by varying defense innovation trajectories, priorities, and resources. In order to project the varying trajectories, it is necessary to conceptualize a comparative framework for defense innovation that integrates the varying stages, paths, and patterns. To begin with, conceptualizing emerging technologies into military capabilities involves internal processes of military innovation as well as external benchmarking processes of adaptation or emulation.[9] A disruptive military innovation may not always require simultaneous technological, doctrinal, and organizational breakthroughs, but may span the spectrum between incremental modernization and discontinuous transformation. Based on these assumptions, one can triangulate defense innovation trajectories along three axes:

1. *conceptual paths*—emulation, adaptation, and innovation;
2. *technological patterns*—speculation, experimentation, and implementation; and
3. *organizational change*—exploration, modernization, and transformation.[10]

Defense emulation paths involve importing new tools and ways of warfare through imitation of other military organizations. Adaptation is defined through adjustments of existing military means and methods, in which multiple adaptations over time may lead to innovation. Defense innovation then involves developing broader military-relevant technologies, tactics, strategies, and structures. Farrell and Terriff observe that "it is only when these new military means and methods result in new organizational goals, strategies, and structures that innovation, adaptation, and emulation lead to major military change."[11] Similarly, according to Thomas Mahnken, military innovation may occur in three distinct but often overlapping phases: (1) speculation; (2) experimentation; and (3) implementation.[12] The speculation phase can be defined through novel ways for solving existing operational problems or acknowledging the potential of emerging technologies. As speculation turns into greater awareness, military services establish experimental organizations, battle laboratories, and units tasked with experimenting with new concepts, force structures, weapons technologies, and warfare methods. With the broadening and deepening experimentation processes a consensus emerges, when the military leadership and services decide to adopt, adapt, and later refine selected experimental operational concepts, warfare methods, organizational force structures, or new generations of weapons systems and technologies. The implementation phase is evident in a range of indicators: i.e. the establishment of new military formations; doctrinal revision to accommodate new ways of war; resource allocation supporting new concepts; development of formal transformation strategy; establishment of innovative military units; new branches and career paths; and ultimately, field training exercises with new doctrine, organizations, or technologies.[13]

In this context, one of the key sets of variables in the matrix is the level and sophistication of a country's defense-innovation ecosystem, which can be defined by a range of "hard" and "soft" innovation capabilities: from technological research and development (R&D) facilities and innovation clusters to non-technological factors such as political, institutional, relational, social, and ideational factors.[14] Together, these factors shape the relative

Figure 2. Conceptualizing Defense Innovation Trajectories.



Source: Michael Raska and Richard Bitzinger, "Locating China's Place in the Global Defense Economy," In Forging China's Military Might: A New Framework for Assessing Innovation, ed. Tai Ming Cheung (Baltimore, MD: Johns Hopkins University Press, 2013); Thomas Mahnken, "Uncovering Foreign Military Innovation," Journal of Strategic Studies 22, no. 4 (1999): 26–54; Theo Farrell and Terry Terriff, eds., The Sources of Military Change: Culture, Politics, Technology (London: Lynne Rienner 2002), 3–21; Andrew Ross, "On Military Innovation: Toward an Analytical Framework," SITC Policy Brief no. 1 (January 2010), 4–17, available at <https://escholarship.org/uc/item/3d0795p8>; Keith Krause, Arms and the State: Patterns of Military Production and Trade (Cambridge, Cambridge University Press, 1992), 12–80.

level of states' indigenous capabilities for independent defense-related R&D, science and technology (S&T) programs, manufacturing, and communities supporting innovation. The varying defense innovation ecosystems can be then broadly structured into three categories: Tier 1A/1B "critical innovators" at the technological frontier of defense production; Tier 2A/B of "adapters and modifiers" of advanced military-related technologies; and Tier 3 of "copiers" and "reproducers" of existing defense technologies.[15] By triangulating defense innovation paths and patterns, it is possible to ascertain the magnitude of organizational change in three stages: (1) exploration, (2) modernization, and (3) transformation.[16] Exploration includes both speculation and emulation, with initial attempts to develop new areas of technological expertise; modernization involves continuous upgrades or improvements of existing military capabilities through the acquisition of new imported or indigenously developed weapons systems and supporting assets.[17] Transformation can be then characterized in the context of a "discontinuous" or "disruptive" defense innovation that meets long-term policy and strategy.

China's Quest for Innovation

The Chinese defense, science, technology, innovation, and industrial base has made undeniable advancements over the past decade and a half in terms of developing and manufacturing new,

relatively modern military systems that increasingly meet the widening operational requirements of the Peoples Liberation Army (PLA). Its progress has reflected Chinese military modernization strategy in a "double construction" approach of mechanization and "informatization" in order to concurrently upgrade and digitize the PLA.[18] This "two-track" approach has called for both the near-term "upgrading of existing equipment combined with the selective introduction of new generations of conventional weapons"—a so-called "modernization-plus" approach—together with a longer-term "transformation" of the PLA along the lines of the information technologies-led Revolution in Military Affairs.[19] In the process, China's long-term strategic military-technological programs have been deeply integrated with its advancing civilian science and technology base, which has been concurrently linked to global commercial and scientific networks.[20] In this context, China is continuously benchmarking emerging technologies and similar high-tech defense-related R&D programs in the United States, Russia, India, Japan, Israel and other countries.[21]

The key aim is to accelerate China's "absorptive capacity" to recognize, assimilate, and utilize external knowledge in the development of China's advanced technologies in both civil and military domains.[22] China calls this strategy "Indigenous Innovation"—first set in the "2006-2020 Medium- and Long-Term Defense Science and Technology Development Plan."[23] By pursuing Indigenous Innovation, China aims to circumvent the costs of research, overcome international political constraints and technological disadvantages, and "leapfrog" China's defense industry by leveraging the creativity of other nations. This includes exploitation of open sources, technology transfer and joint research, the return of Western-trained Chinese students, and, of course, industrial espionage, both traditional and increasingly, cyber-exploitation—i.e. systematic hacking.[24]

Notwithstanding these efforts, however, the Chinese arms industry still appears to possess only limited indigenous capabilities for cutting-edge defense R&D. Western armaments producers continue to outpace China when it comes to most military technologies, particularly in areas such as propulsion (aircraft/missile engines), navigation systems and defense electronics, and high-end composites. In retrospect, the confluence of historical legacies of centralized planning coupled with segmented technological, institutional, and management deficiencies such as overlapping planning structures, widespread corruption, bureaucratic fragmentation, problems with quality control, manufacturing, and process standardization have precluded the Chinese military-industrial conglomerates from leaping ahead on the innovation ladder. Most importantly, no real internal competition exists and the industry lacks sufficiently capable R&D and capacity to develop and produce highly sophisticated conventional arms. Confronting these challenges, China has progressively introduced a series of medium-and long-term defense industrial strategies, plans, and institutional reforms that have generally set two broad strategic objectives known as "two gaps:"

- to catch-up with the global military-technological state-of-the-art base by fostering "indigenous innovation," mitigate foreign dependencies on technological transfers and arms imports, while leveraging civil-military integration to overcome entrenched barriers to innovation; and
- to provide advanced weapons platforms, systems, and technologies that would enable the PLA's transformation into a fully "informatized" fighting force—one capable of conducting sustained joint operations, military operations other than war, and missions

related to China's strategic deterrence to protect China's core national security interests beyond national borders.[25]

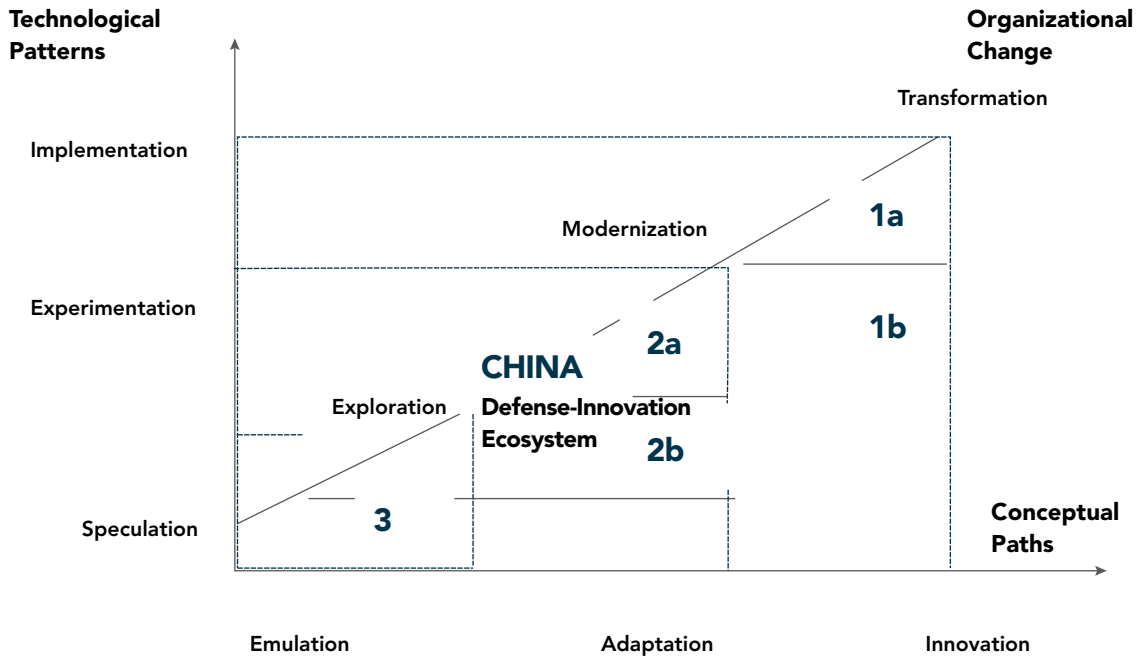
Under Xi Jinping, China's strategy to resolve both gaps has focused principally on upgrading civil and military convergence. In particular, since 2003, the conceptual umbrella for leveraging civil military integration (CMI) became known as *Yujun Yumin*—locating military potential in civilian capabilities—signifying transfer of commercial technologies to military use, and calling upon the Chinese arms industry not only to develop dual-use technologies, but also actively promote joint civil-military technology cooperation. Yujun Yumin has been prioritized in the 2004 Defense White Paper, subsequent Five-Year Defense Plans, as well as in the 2006–2020 Medium- and Long-Term Defense Science and Technology Development Plan (MLP).[26] Select dual-use technology development areas, for example, included microelectronics, space systems, new materials (such as composites and alloys), propulsion, missiles, computer-aided manufacturing, and particularly information technologies.[27]

Initially, China's political establishment envisioned CMI as institutional arrangements paving the way for a new round of associated management reforms for the defense industry, including allowing select civilian private sector firms to engage in defense work. These in turn would enable expanding linkages and collaboration between China's military-industrial complex and civilian high-technology R&D sectors. In 2016, however, President Xi Jinping elevated CMI into a national-level strategy noting that "the integration of civilian and defense development will involve multiple fields and enable economic progress to provide a 'greater material foundation' for defense construction, while the latter offers security guarantees for the former."[28] In other words, CMI has been projected not only as a key enabler to PLA's military-technological modernization, but more importantly, as a strategy for China's long-term sustainable growth, efficiency and productivity gains, as well as mitigating internal socio-economic and environmental challenges. Currently, CMI as a national strategy expands the integration of state-owned defense research, development, and manufacturing enterprises, government agencies under the State Council, universities, and private sector firms in order to advance the PLA's military modernization, while supporting China's economic growth.[29] In this context, China has created new agencies in 2017 such as the Central Commission for Integrated Military and Civilian Development and the Scientific Research Steering Committee, both tasked to advance the R&D of state-of-the-art weapons platforms and systems.[30]

At the same time, China's CMI places strategic importance on foreign acquisition of dual-use technologies, resources, and knowledge in selected priority areas identified in recent defense science and technology plans—such as the "13th Defense Science and Technology (S&T) and Industry Five-Year Plan;" "2025 Defense Science and Technology Industry Plan;" and the "Made in China 2025" advanced manufacturing plan.[31] According to the 2015 *China Military Strategy*, "China will work to establish uniform military and civilian standards for infrastructure, key technological areas and major industries, explore the ways and means for training military personnel in civilian educational institutions, developing weaponry and equipment by national defense industries, and outsourcing logistics support to civilian support systems."[32] In this context, China aims to achieve military advantage from key emerging technologies such as quantum computing and communications, hypersonics, artificial intelligence, big data applications, cloud computing, 3D printing, nanomaterials, and biotechnology by creating a modernised defence industrial base that leverages civil and military convergence.[33]

In short, the evolving strategy of Indigenous Innovation in a broader context of civil-military

Figure 3. China's Defense Innovation Trajectories.



Source: Michael Raska and Richard Bitzinger, "Locating China's Place in the Global Defense Economy," In Forging China's Military Might: A New Framework for Assessing Innovation, ed. Tai Ming Cheung (Baltimore, MD: Johns Hopkins University Press, 2013).

integration constitutes a pathway for China's long-term strategic competition.[34] In doing so, China continues to seek niche technological developments that could potentially revolutionize the PLA's military operations by providing a credible asymmetric edge in regional flashpoints in East Asia: i.e. anti-ship ballistic missiles (ASBMs), anti-satellite ballistic missiles, hypersonic cruise missiles, and systems converging cyber and space capabilities. Notwithstanding military-technological trajectories, China's military effectiveness will be increasingly influenced by its ability to align its political and strategic goals with technological advancements. This includes China's ability to alter strategic alliances and balance of power through international arms exports, technology transfers, and military cooperation. Overall, China is still more of a "fast follower," always playing technology "catch-up," or else a niche innovator when it comes to military R&D. Additionally, it may be acceptable to be a niche innovator if the military is only looking to gain asymmetric niche advantages, such as the PLA using an ASBM to attack aircraft carriers.[35] Ultimately, transforming emerging technologies into actual capabilities will be shaped by the PLA's ability to integrate novel technologies to joint military concepts.[36]

Russia's Return to First Offset

Russia has been closely monitoring the United States as well as China's technological priority areas, while assessing its long-term consequences, and searching for means to counter them.[37] In this context, Russian strategy has broadly consisted of two major elements: The first one is "countering the Third Offset Strategy with the First Offset Strategy," which means prioritizing the development of a wide

array of both strategic and tactical nuclear weapons systems. In Russian strategic thought, maintaining a variety of sophisticated nuclear weapons can invalidate any conventional advantages of the United States, NATO, and China. Ensuring that Russia remains a nuclear superpower is the basis of all Russian security policies. Moscow has never ceased the development of strategic and tactical weapon systems even during the darkest days of 1990s, and indeed accelerated research and development during the period of swift economic growth in the 2000s. Russia sees nuclear weapons as the most cost-effective pillar of strategic deterrence. The Strategic Rocket Forces, the service that controls the Russian ground based ICBMs and serves as the main component of the Russian strategic nuclear triad, accounts for a mere 5 percent of defense expenditures.[38]

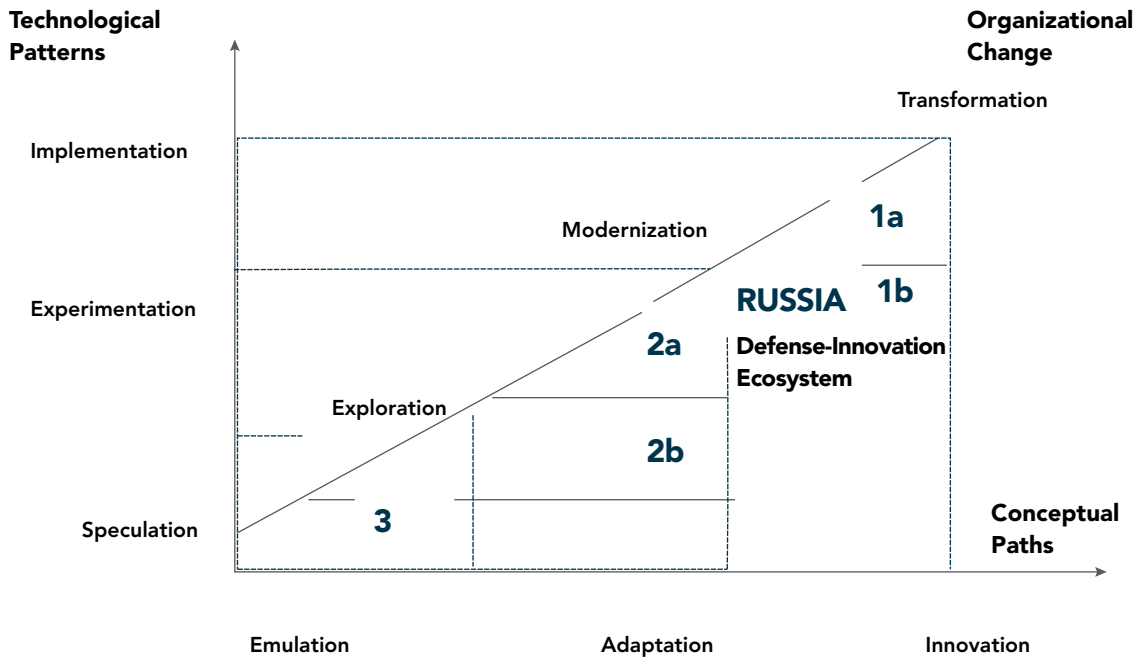
Notwithstanding Russia's recent economic downturn and defense expenditure cuts, select major nuclear-related projects continue to expand. For example, Russia has been deploying the new RS-24 *Yars* (SS-27 Mod 2) ICBMs, and the new *Borei* class SSBNs armed with RSM-56 *Bulava* (SS-N-32) missile systems. Simultaneously, however, Russia has been developing at least two additional ICBM families: a heavy liquid fuel *Sarmat* ICBM (RS-28) and a mobile solid fuel *Rubezh* (RS-26) system, specifically designed to defeat future U.S. missile defense shields in Europe. The development of a rail-based ICBM system utilizing one of the existing ICBM types (most likely RS-24) has also begun. Furthermore, Russia is working on hypersonic reentry vehicles for its ICBMs.[39] Another extensive program is the development of a significantly upgraded version of the *Tu-160 Blackjack* strategic bomber, which will be produced in Kazan. Moscow takes any possible threat to the effectiveness of Russian nuclear forces very seriously, and immediately embarks on planning countermeasures. In 2015, the Russian state-run TV, reporting on a policy meeting in the Kremlin, revealed, most likely intentionally, the existence of a bizarre strategic weapons project called *Status-6*—a 10,000+ km range nuclear-powered torpedo, capable of travelling at the depth of 1,000 meters at great speeds. The stated purpose of this weapon is to destroy coastal cities and installations with nuclear warheads, although different types of payload are also a possibility.[40]

Russia continues to develop and deploy a wide range of tactical nuclear weapons, including nuclear-capable cruise missiles, nuclear bombs, nuclear-capable SAM missiles for long-range SAM systems, nuclear torpedoes, and nuclear versions of short-range ballistic missiles. These projects, especially the rearmament of ten missile brigades of the Russian Army with the *Iskander* (SS–26 Stone) short-range missile systems, are also high priority.[41] Some of the Russian countermeasures are rather unique. Russia is the only country in the world which deploys medium-range cruise missiles (*Kalibr*, SS–N–30A) on small (less than 1,000 tons of displacement) corvettes. Such ships belonging to the existing *Buyan-M* and the future *Karakurt* classes are estimated to be produced in significant numbers. The *Buyan-M* corvettes were combat-tested as cruise missile carriers in the Syrian campaign as well as the new Russia project 636.3 (*Improved Kilo*) conventional submarines. Other delivery systems, including SS–26, Su–34 tactical bombers, and the new air-launched cruise missiles have also been combat-tested during the Syrian war. In short, Russia's programs focusing on rearmament of the nuclear forces are progressing into advanced stages. Russia already has a significant advantage over the U.S. in terms of the quality and variety of its delivery systems, and can reasonably ensure the strategic effectiveness of its nuclear forces in the near future.

The second element in Russia's strategy is more ambitious, carrying broader technological risks. Russia began to counter many U.S. and Chinese technological initiatives using similar indigenous programs, although more narrowly focused and

smaller in scale. In October 2012, Russia established the Advanced Research Foundation (ARF)—a counterpart to the U.S. DARPA (Defense Advanced Research Projects Agency). The ARF focuses on R&D of high-risk, high-pay-off technologies in areas that include hypersonic vehicles, artificial intelligence, additive technologies, unmanned underwater vehicles, cognitive technologies, directed energy weapons, and others. While Russian technologies are at the early stages in some areas, in key areas such as directed energy weapons, rail gun, hypersonic vehicles, and unmanned underwater vehicles, programs are progressing into advanced stages, backed by considerable financing for many years prior to the ARF.[42] The key challenge for Russia, however, is sustained resource allocation to translate these "disruptive" innovations into actual military capabilities.[43] Since Russian resources are limited and its political relations with the West are unlikely to be normalized anytime soon, it is possible that Russia will try to establish new industrial partnerships with major non-Western countries such as India and China to secure financing and technological cooperation on these projects. Russia has already had a positive experience with India (*BrahMos* cruise missile joint production venture), and has embarked on two major joint programs with the Chinese—a wide-body passenger aircraft and advanced heavy helicopter programs. The interest in establishing the new joint programs with the Chinese is especially strong in the Russian space industry. The purchase of Chinese space-grade microchip production technology in exchange for RD–180 liquid-fuel rocket engine technology is under negotiation, and may start a new stage in Sino–Russian cooperation.

Figure 4. Russia's Defense Innovation Trajectories.



Source: Framework based on Michael Raska and Richard Bitzinger, "Locating China's Place in the Global Defense Economy," In Forging China's Military Might: A New Framework for Assessing Innovation, ed. Tai Ming Cheung (Baltimore, MD: Johns Hopkins University Press, 2013).

U.S. Defense Innovation Advances and Challenges

The U.S. defense community is debating a range of capability requirements and top priority investments that will shape U.S. strategy and the use of force in the 21st century. While mapping all major initiatives, concepts, and programs would transcend the scope of this article, one could argue that the U.S. Department of Defense (DOD) seeks to develop technologically enabled novel operational and organizational constructs that would sustain U.S. military superiority over its capable adversaries at the operational level of war, thereby strengthening conventional deterrence. One particular element, often emphasized by the DOD, is the importance of "institutional agility"—or improving the ability to out-innovate adversaries, rethink how the DOD sources technology and rethink its models for product delivery. In recent years, the DOD has aimed to streamline its science and technology engines, or S&T enterprises to support sustained research in fundamental technologies and quickly leverage emerging technical opportunities in the commercial sector, including cyber. In doing so, the DOD has aimed to use all potential sources of technical advantage, from traditional industrial base, non-traditional suppliers, and academia to help create competitive advantage by means of translating technical capabilities into solutions and concepts that would turn into capabilities to overmatch any threat. During the Obama Administration, these efforts were embedded in the concept of the *Third Offset Strategy*. The strategy became public in the 2014 Defense Innovation Initiative (DII), which was presented as a comprehensive effort for the U.S. defense community to search for innovative ways to sustain and advance U.S. military superiority in an era in which U.S. dominance in key warfighting domains has been eroding, while facing constrained and uncertain budgets.[44] The DII called for a revamped institutional agility that would accelerate U.S. military innovation in select areas, including leadership and defense management, long-range research and development programs to identify, develop, and field breakthrough technologies, a reinvigorated war-gaming effort to develop and test alternative ways of achieving strategic objectives, and novel operational concepts to employ resources to greater strategic effect. Similarly, the Third Offset Strategy sought to conduct numerous "small bets" on advanced capability research and demonstrations, while working to craft new operational concepts to determine capability requirements and top priority investments that will shape U.S. military strategy in the 21st century.[45]

While the Trump Administration discarded the term Third Offset, its programs and priorities have arguably continued, aiming to exploit technologies of the Fourth Industrial Revolution to attain and prolong the margin of the U.S. technological superiority that may bring unprecedented military capabilities.[46] These include leveraging learning machines—integrating artificial intelligence and autonomy into an advantage; i.e. instantly responding against cyber-attacks, electronic attacks, or attacks against space architecture or missiles; human-machine collaboration—using advanced computers and visualization to help people make faster, better, and more relevant decisions; assisted human operations—plugging every pilot, soldier, sailor, and marine into the battle network; human-machine combat teaming—creating new ways for manned and unmanned platforms to operate; and network-enabled autonomous weapons—weapons platforms and systems plugged into a learning command, control, communications, and intelligence, or C3I, network. Other "hidden" priority areas associated with emerging technologies have also been cited in the context of cross-domain strategic deterrence capabilities, particularly converging nuclear and cyber deterrence.[47]

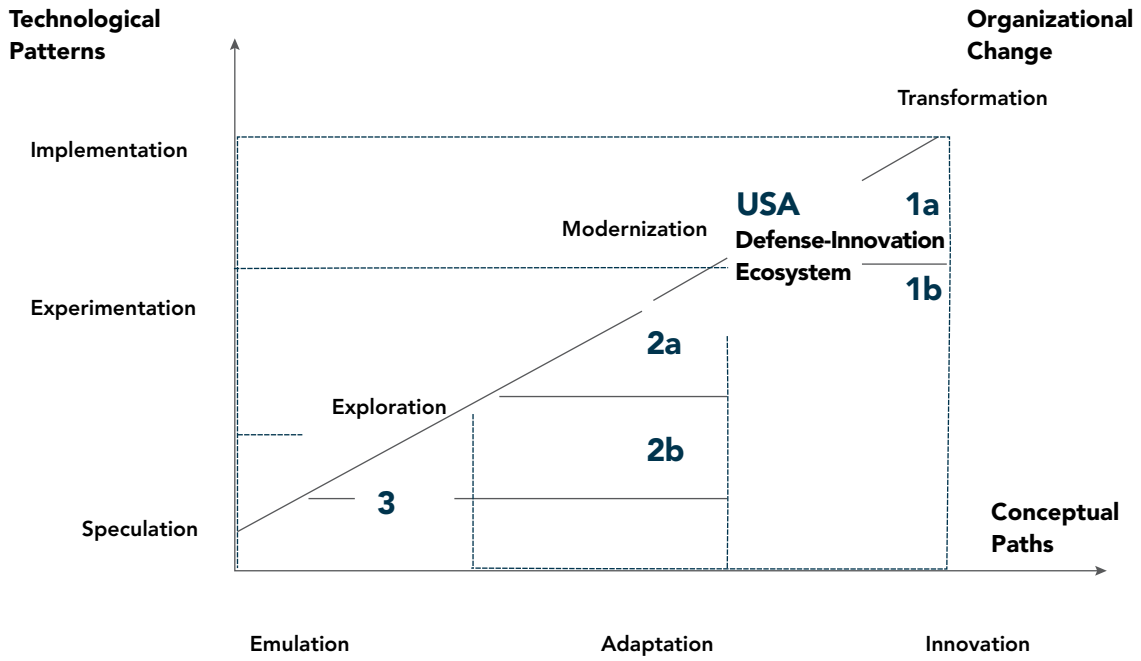
Overall, the United States continues its military innovation lead in terms of future-oriented

technological patterns, conceptual paths, however, with relatively slow organizational adoption and adaptation. Strategic effectiveness of U.S. military innovation, however, will not only depend on the institutional agility and adoption capacity—the financial intensity and organizational capital required to adopt military innovations—but will also depend on the responses, resources, and counter-innovations by peer competitors. Notwithstanding the diffusion and convergence of novel technologies—electronic miniaturization, additive manufacturing, nano-technology, artificial intelligence, space-like capabilities, and unmanned systems that are likely to alter the character of conflict over time—the patterns of "challenge, strategic response, and adaptation" will continue to shape the direction and character of long-term strategic competitions.

Strategic Implications

In the 21st century, China, Russia, and the United States continue to pursue the development, acquisition, deployment, and exercising of new technologies as means to create advantages and influence events or the strategic choices of their competitors.[48] According to a recent study, there are four distinct but mutually-supporting competitive strategies: (1) strategies of denial; (2) cost imposing strategies; (3) attacking a competitor's strategy; and (4) attacking a competitor's political system.[49] Denial strategies seek to prevent an opponent from attaining political objectives by demonstrating military-technological capability to convince an opponent that a particular action such as an aggression cannot be successful. Cost-imposing strategies, meanwhile, aim to convince a competitor that the cost of a particular course of action is prohibitively

Figure 5. U.S. Defense Innovation Trajectories.



Source: Framework based on Michael Raska and Richard Bitzinger, "Locating China's Place in the Global Defense Economy," In Forging China's Military Might: A New Framework for Assessing Innovation, ed. Tai Ming Cheung (Baltimore, MD: Johns Hopkins University Press, 2013).

high, and in doing so, dissuade or deter competitors from taking a certain action. At the same time, such strategies seek to divert competitors' resources across seemingly important, but strategically non-essential economic, political, and military arenas. The third approach, attacking a competitor's strategy, seeks to narrow competitors' strategic choices into a virtually self-defeating behavior. Historical examples include the development of the U.S. AirLand Battle doctrine in the 1970s and 80s that convinced the Soviet Union of its inability to implement its preferred strategy. Currently, China's counter-intervention or anti-access/area-denial (A2/AD) strategy similarly aims to attack and negate the effectiveness of U.S. power projection strategies in East Asia. Finally, strategies attacking a competitor's political system seek to exploit subversive factions within that system. For example, during the Cold War, the U.S. Strategic Defense Initiative (SDI) amplified debates within Soviet leadership over the direction, character, and strategic utility to compete with the United States in space development.[50]

The character of the ongoing strategic competition suggests the presence of all four above-mentioned competitive strategies. Yet, there are contending debates and varying policy vistas with regard to the most fundamental aims, objectives, and motives that entangle the great powers in strategic competition. Central to these debates are questions including to what degree do China, Russia, and the United States aim to maximize the share of relative hard power as a means to attain their security, status, and influence to achieve geopolitical outcomes; whether economic interdependencies assure stability, peace, and prosperity, rather than amplifying economic competition that increases resource insecurity and the propensity for China and the United States to seize access and control of resources; whether territorial, maritime, and other border disputes coupled with more strident forms of nationalism have the potential to become more escalatory; whether the diffusion of ideological values, visions, and cultural preferences creates shared identity leading to cooperation or rather does it reflect a mirage of political, economic, and perhaps even ideological cohesion; and ultimately, whether multilateral institutions and norms converge global or regional security interests and lasting peace, or encourage great powers to seek control of the agenda, rules, and norms of international institutions to shape the prevailing order?[51]

The resurgence of great power rivalries, particularly notable in East Asia, coupled with intensifying arms competition for advanced military technologies suggests that while wars and conflicts are not inevitable, neither are they inconceivable. In potential military confrontations, however, between adversaries armed with substantial nuclear arsenals and stand-off precision strike systems, there are considerable escalatory risks. Accordingly, great powers are engaging in competitive strategies to avoid large-scale wars of attrition, and instead rely on "peacetime" non-military diplomatic, information, and economic actions coupled with paramilitary operations to gain influence and territory without having to escalate to a major conflict.[52] These "indirect" actions can include the use of information operations and political warfare, cyber-attacks, electronic warfare, as well as paramilitary operations in disputed areas. The progressive complexity of cyber and information operations is reflected in cross-domain strategic interactions, between cyber, physical, and cognitive information domains, civil and military spheres, and involving both state and non-state actors.[53] These include confrontations in and out of cyberspace, cyberattacks on physical systems and processes controlling critical information infrastructure, information operations, and various forms of cyber espionage. Accordingly, nearly all great powers are developing advanced cyber capabilities—whether defensive, offensive, or intelligence-driven—which are increasingly used

as instruments of warfare—as a key enabler and force-multiplier of "kinetic" operations—enabling actions, capabilities, and effects in land, sea, air, space, and intelligence operations in all domains.

The resulting progressive complexity in strategic interactions and interdependencies between cyber, information, cognitive, and physical domains presents new challenges to traditional conceptions.[54] of the uses of force. In particular, the convergence of both military and non-military instruments of warfare through cyber and information means brought about through emerging technologies is often viewed in the context of two inter-related strategic challenges: (1) "cross-domain deterrence and compellence" (CDD&C); and (2) asymmetric anti-access/area-denial challenges—with both having significant impact on the character of warfare, particularly in East Asia. CDD&C refers to the act of deterring an action in one domain with a threat in another domain, where the domains are defined as land, under the land, at sea, under the sea, in the air, in space, and in cyberspace, and may often use economic sanctions and other diplomatic, political, and informational tools. In this context, CDD&C may leverage both deterrence—dissuading an actor from taking an action before they act; and coercive diplomacy—persuading an actor to stop a particular course of action after they initiated action. In other words, cross-domain coercion uses threats of force in multiple domains to influence an opponent's strategic choices.[55]

Consequently, when contemplating how emerging technologies may affect East Asian security and defense requirements, militaries in the region will need to explore the nature of the evolving strategic competition in the region. In particular, U.S. allies and strategic partners in East Asia, including Japan, South Korea, and Singapore, will have to plan for potential U.S. involvement in emerging conflicts in the East China Sea and South China Sea vis-à-vis China: what types of challenges does this present for them? How will they operate in a contested environment characterized by the diffusion of sophisticated longer-range adversary capabilities and methods such as ballistic missiles, submarines, weapons of mass destruction, and offensive space and cyberspace assets? At the same time, however, the character of future conflicts in the regional "gray zones" may also reflect low-intensity conflicts in "peripheral campaigns," rather than high-end missions—given the considerable escalatory risks. In a context where the battle space is crowded with both legally constituted combatants and non-combatants, this will present new challenges. Consequently, military-technological advantages will not be effective without corresponding *strategic, organisational and operational adaptability*—not only detecting new sources of military innovation, but also, changing military posture quickly and easily in response to shifts in geostrategic environment, military technology, resource allocation, organisational behaviour, and national priorities.[56]

Ultimately, the diffusion of emerging technologies shaping military innovation trajectories must be viewed in a relative context—through the lens of *competitive strategies* reflected in the efforts to develop effective counter-measures and responses. A key requirement will be the capacity of the select militaries to educate both the officer corps and the rank-and-file on the changing character of war, and what the laws of armed conflict permit military personnel to do. Under the conditions of strategic ambiguity, regional militaries will therefore have to redefine their "theories of victory." Taken together, new technologies will increasingly shape strategic choices in the 21st century, including defense planning, management, and technological priorities, propelling the need for strategic and operational adaptation and innovation to prepare for, fight, win, and deter new types of conflicts. PRISM

Notes

[1] Michael J. Mazarr et all, "Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives," RAND Research Report

2726 (Santa Monica, CA: RAND Corporation, 2018), available at <https://www.rand.org/pubs/research_reports/RR2726.html>.

[2] The White House, *The National Security Strategy 2017* (Washington D.C.: The White House, 2017), available at <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>; and Department of Defense, *The National Defense Strategy* 2018 (Washington D.C.: Office of the Secretary of Defense, 2018), available at <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

[3] Aaron Friedberg, "Competing with China," *Survival* 60, no. 3 (June 2018), available at <https://www.iiss.org/pubilcations/survival/2018/survival-global-politics-and-strategy-junejly-2018/603-02-friedberg>.

[4] Robert Work, "The Third U.S. Offset Strategy and its Implications for Partners and Allies," January 28, 2015, available at <https://dod.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/>.

[5] Chung Min Lee, *Fault Lines in a Rising Asia* (Washington D.C.: Carnegie Endowment for International Peace, 2016), 190.

[6] Thomas Mahnken, "Thinking about Competitive Strategies," *In Competitive Strategies for the 21st Century: Theory, History, and Practice*, ed. Thomas Mahnken (Stanford, CA: Stanford University Press, 2012), 6.

[7] Thomas Mahnken, "A Framework for Examining Long-Term Strategic Competition Between Major Powers," *SITC Research Brief*, January 2017, available at<https://escholarship.org/uc/item/0754362r>.

[8] T.X. Hammes, "Technologies Converge, Power Diffuses," Paper presented at RSIS-TDSI Seminar "Disruptive Defence Technologies in Military Operations," Singapore, June 29, 2016, available at <https://www.rsis.edu.sg/wp-content/uploads/2016/08/ER160823_RSIS-TDSI.pdf>.

[9] Terry Terriff, Frans Osinga, and Theo Farrell, eds., *A Transformation Gap? American Innovations and European Military Change* (Palo Alto, California: Stanford University Press, 2010).

[10] Andrew L. Ross, "On Military Innovation: Toward an Analytical Framework," SITC Policy Brief no. 1 (January 2010), 14–17, available at <https://escholarship.org/uc/item/3d0795p8>; Theo Farrell and Terry Terriff, eds., *The Sources of Military Change: Culture, Politics, Technology* (London: Lynne Rienner 2002), 3-21.; Thomas Mahnken, "Uncovering Foreign Military Innovation," *Journal of Strategic Studies* 22, no. 4 (1999): 26–54; Michael Raska, "RMA Diffusion Paths and Patterns in South Korea's Military Modernization," *Korean Journal of Defense Analyses* 23, no.3 (2011), 369–385.

[11] Farrell and Terriff, eds., *The Sources of Military Change: Culture, Politics, Technology*, 6.

[12] Thomas Mahnken, "Uncovering Foreign Military Innovation," 31.

[13] Ibid, 31–34.

[14] Tai Ming Cheung, "The Chinese Defense Economy's Long March from Imitation to Innovation," *Journal of Strategic Studies* 34, no.3 (17 June 2011), 325–54.

[15] Keith Krause, *Arms and the State: Patterns of Military Production and Trade* (Cambridge, Cambridge University Press, 1992), 12–80.

[16] Andrew Ross, "On Military Innovation: Toward an Analytical Framework," SITC Policy Brief no. 1 (January 2010), 14–17, available at <https://escholarship.org/uc/item/3d0795p8>.

[17] Michael Wills and Ashley J. Tellis, eds., *Strategic Asia 2005-06: Military Modernization in an Era of Uncertainty* (Seattle, WA: The National Bureau of Asian Research, 2005), 15.

[18] You Ji, "China's Emerging National Strategy," *China Brief*, November 24, 2004.

[19] Tai Ming Cheung, "Dragon on the Horizon: China's Defense Industrial Renaissance," *Journal of Strategic Studies*, 32, no. 1 (February 2009), 30–31.

[20] Michael Raska, "Scientific Innovation and China's Military Modernization," *The Diplomat*, September 3, 2013.

[21] DOD Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2013).

[22] Tai Ming Cheung, "The Chinese Defense Economy's Long March from Imitation to Innovation," *Journal of Strategic Studies* 34, No.3 (17 June 2011): 343-344; Scott Kennedy, "Made in China 2025," Center for Strategic & International Studies, June 1, 2015, available at <https://www.csis.org/analysis/made-china-2025>.

[23] Tai Ming Cheung, "The Chinese Defense Economy's Long March from Imitation to Innovation," 343–44.

[24] Jon Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, eds., Jon Lindsay, Tai Ming Cheung, and Derek Reveron, (New York, NY: Oxford University Press, 2015), 66.

[25] Michael S. Chase, Jeffrey Engstrom, Tai Ming Cheung, et.al., *China's Incomplete Military Transformation Assessing the Weaknesses of the People's Liberation Army* (Washington D.C.: RAND Corp., 2015), 69; and You Ji, *China's Military Transformation: Politics*

and War Preparation (Cambridge, UK: Polity Press, 2016).

[26] Central People's Government of the People's Republic of China, "*China Issues S&T Development Guidelines*, February 9, 2006, available at <http://www.gov.cn/english/2006-02/09/content_183426.htm>; Eric Hagt, "Emerging Grand Strategy for China's Defense Industry Reform," in *The PLA at Home and Abroad: Assessing the Operational Capabilities of China's Military*, eds. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: U.S. Army War College, 2010), 481–84.

[27] Tai Ming Cheung, ed., *Forging China's Military Might: A New Framework for Assessing Innovation* (Baltimore, MD: Johns Hopkins University Press, 2013).

[28] Xinhua News, "Xi Urges Deeper Military-Civilian Integration," October 16, 2018, available at <http://www.xinhuanet.com/english/2018-10/16/c_137534739.htm>; Xinhua News, "China Focus: Xi Stresses Integrated Military, Civilian Development," September 22, 2017, available at <http://www.xinhuanet.com/english/2017-09/22/c_136630454.htm>.

[29] Greg Levesque and Mark Stokes, *Blurred Lines: Military-Civil Fusion and the 'Going Out' of China's Defense Industry* (Washington D.C.: Pointe Bello, 2016).

[30] Zhao Lei, "Civil-Military Integration will Deepen," *China Daily*, March 3, 2018, available at <http://www.chinadaily.com.cn/a/201803/03/WS5a99d67ca3106e7dcc13f437.html>; Minnie Chan, "Chinese Military Sets-up Hi-tech Weapons Research Agency Modelled on US Body," *South China Morning Post*, July 25, 2017, available at <https://www.scmp.com/news/china/diplomacy-defence/article/2104070/chinese-military-sets-hi-tech-weapons-research-agency>.

[31] Tai Ming Cheung et al., "Planning for Innovation—Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," report prepared for the U.S.-China Economic and Security Review Commission, July 28, 2016, available at <https://www.uscc.gov/Research/planning-innovation-understanding-china%E2%80%99s-plans-technological-energy-industrial-and-defense>.

[32] Information Office of the State Council of the People's Republic of China, "*China's National Defense in 2015*," May 26, 2015, available at <http://eng.mod.gov.cn/Database/WhitePapers/index.htm>.

[33] Tai Ming Cheung, "The Chinese Defense Economy's Long March from Imitation to Innovation," *Journal of Strategic Studies* 34, no.3 (June 17, 2011): 343-344; Scott Kennedy, "Made in China 2025," Center for Strategic & International Studies, June 1, 2015, available at <https://www.csis.org/analysis/made-china-2025>.

[34] Tai Ming Cheung et al., "Chinese Defense Industry Reforms and Their Implications for US-China Military Technological Competition," *Study of Innovation and Technology in China Research Brief* (San Diego, CA: University of California Institute on Global Conflict and Cooperation, January 4, 2017), available at <https://escholarship.org/uc/item/84v3d66k>.

[35] Richard Bitzinger and Michael Raska, "Capacity for Innovation: Technological Drivers of China's Future Military Modernization," in *The Chinese People's Liberation Army in 2025*, eds. Roy Kamphausen and David Lai (Carlisle, PA: Strategic Studies Institute, 2015), available at <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1276>.

[36] Cortez A. Cooper, "PLA Military Modernization Drivers, Force Restructuring, and Implications," Testimony presented before the U.S.–China Economic and Security Review Commission, February 15, 2018, available at <https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT488/RAND_CT488.pdf>.

[37] Michael Raska and Vasily Kashin, "Countering the U.S. Third Offset Strategy: Russian Perspectives, Responses and Challenges," *RSIS Policy Report*, January 24, 2017, available at <https://www.rsis.edu.sg/rsis-publication/idss/countering-the-u-s-third-offset-strategy-russian-perspectives-responses-and-challenges/#.W48_Iugza71>.

[38] "Statement by the former Chief of Staff of the Russian Strategic Rocket Forces Gen. Victor Esin—Press Conference," Interfax.Ru, February 15, 2014, available at <http://www.interfax.ru/presscenter/360999>.

[39] "В России испытали гиперзвуковой управляемый боевой блок для баллистических ракет (Russia has tested a Hypersonic Reentry Vehicle for Ballistic Missilies)," Lenta.Ru, April 21, 2016, available at <https://lenta.ru/news/2016/04/21/agbo/>.

[40] "В Кремле прокомментировали кадры телеканалов с засекреченной системой Статус-6 (Kremilin Comments on TV Channels Reports on the Secret)," Lenta.Ru, November 11, 2015, available at <https://lenta.ru/news/2015/11/11/oops/>.

[41] "20-я гвардейская ракетная бригада получила комплект ракетного комплекса Искандер-М (20th Guards Missile Brigade Receives Iskander-M Missile Systems)," *VPK News*, June 30, 2016, available at <http://vpk.name/news/158502_20ya_gvardeiskaya_raketnaya_brigada_poluchila_komplekt_raketnogo_kompleksa_iskanderm.html>.

[42] Advanced Research Foundation of the Russian Federation Website, "Areas of Work," available at <https://fpi.gov.ru/projects/>.

[43] Michael Raska and Vasily Kashin, "Countering the U.S. Third Offset Strategy:

Russian Perspectives, Responses and Challenges," RSIS Policy Report, January 24, 2017, available at <https://www.rsis.edu.sg/rsis-publication/idss/countering-the-u-s-third-offset-strategy-russian-perspectives-responses-and-challenges/#.W48_Iugza71>.

[44] Timothy Walton, "Security the Third Offset Strategy—Priorities for the Next Secretary of Defense," *Joint Forces Quarterly*, (3rd Quarter 2016), 6–15; Chuck Hagel, "Memorandum—The Defense Innovation Initiative," Office of the Secretary of Defense, Washington D.C., November 15, 2014, available at <https://www.defense.gov/Newsroom/News/Article/Article/603658/>.

[45] Cheryl Pellerin, "Deputy Secretary Discusses Third Offset, First Organizational Construct," *Department of Defense News*, September 21, 2016, available at <http://www.defense.gov/News/Article/Article/951689>.

[46] Cheryl Pellerin, "Work: Human-Machine Teaming Represents Defense Technology Future," *Department of Defense News*, November 8, 2015, available at <http://www.defense.gov/News/Article/Article/628154/work-human-machine-teaming-represents-defense-technology-future>.

[47] Bill Gertz, "Pentagon Developing Pre-Launch Cyber Attacks on Missiles," *The Washington Free Beacon*, April 14, 2016, available at <http://freebeacon.com/national-security/pentagon-developing-pre-launch-cyber-attacks-missiles/>.

[48] Thomas Mahnken, "Thinking about Competitive Strategies," In *Competitive Strategies for the 21st Century*, ed. Thomas Mahnken (Stanford: Stanford University Press, 2012).

[49] Ibid, 2.

[50] Ibid, 3.

[51] Aaron Friedberg, "Warring States: Theoretical Models of Asia Pacific Security," *Harvard International Review*, 18. no.2 (1996), 12-68; Graham Allison, "The Thucydides Trap: Are the U.S. and China Headed for War?" *The Atlantic*, September 24, 2015, available at <https://www.theatlantic.com/international/archive/2015/09/united-states-china-war-thucydides-trap/406756/>; T.J. Pempel, "Security Architecture in Northeast Asia: Projections from the Rearview Mirror," in *Security Cooperation in Northeast Asia: Architecture and Beyond*, eds. Chung-Min Lee and T.J. Pempel (New York, NY: Routledge, 2012), 212-232; Michael J. Mazarr et al., *Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives* (Santa Monica, CA: RAND Corporation, 2018), 33.

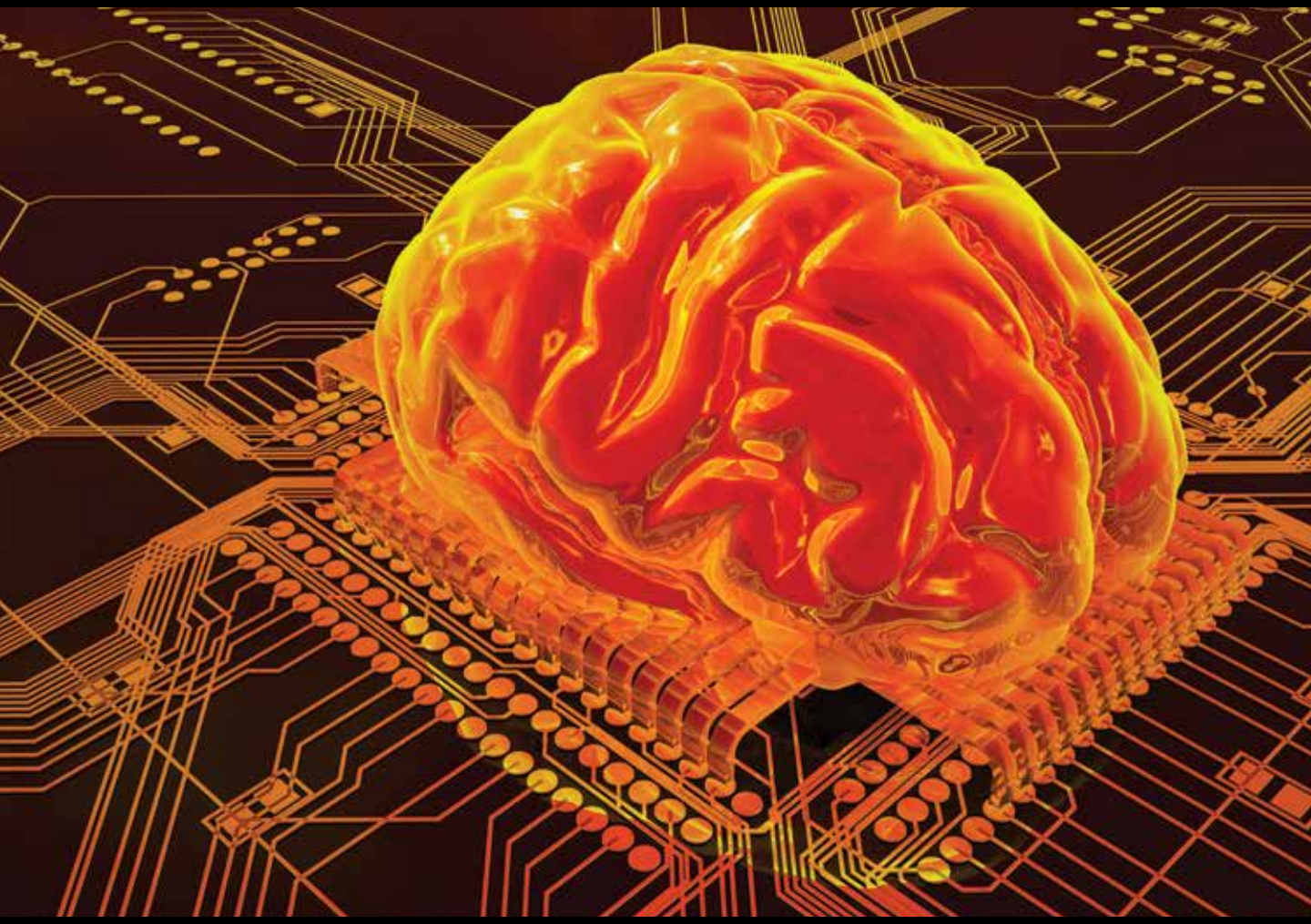
[52] Mark Gunzinger et al., *Force Planning for the Era of Great Power Competition* (Washington D.C.: Center for Strategic and Budgetary Assessments, 2017).

[53] U.S. Joint Staff, *Joint Force Development, Cross-Domain Synergy in Joint Operations: A Planner's Guide* (Washington D.C.: Department of Defense, 2016), available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230>.

[54] U.S. Department of Defense, "Summary: The DoD Cyber Strategy 2018," (Washington D.C.: U.S. Department of Defense, 2018), 1–7, available at <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>.

[55] Mallory King, "New Challenges in Cross-Domain Deterrence," *RAND Perspective*, no. 259 (2018), available at <https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE259/RAND_PE259.pdf>.

[56] Paul Davis, "Defence Planning in an Era of Uncertainty: East Asian Issues," in *Emerging Threats, Force Structures, and the Role of Air Power in Korea*, eds. Natalie Crawford and Chung-in Moon (Santa Monica, CA: RAND, 2000), 25–47.



"As the the cognitive demands for commanders are expected to become more acute on the future battlefield, new directions in integrating human and machine intelligence could prove militarily advantageous." (from this article)

Minds at War

China's Pursuit of Military Advantage through Cognitive Science and Biotechnology

By Elsa B. Kania

The United States is starting to confront unprecedented challenges to the military and technological superiority that it has enjoyed in recent history. The People's Republic of China (PRC) is emerging as a powerhouse across a range of emerging technologies, and Chinese leaders recognize today's technological revolution as a critical, even historic, opportunity to achieve strategic advantage.[1] As Chairman of the Central Military Commission (CMC) and Commander-in-Chief of the CMC Joint Operations Center, Chinese Communist Party (CCP) General Secretary Xi Jinping has highlighted the importance of military innovation to "keep pace with the times" (与时俱进) and adapt to the global revolution in military affairs.[2]

Indeed, Xi has declared, "In circumstances of increasingly intense global military competition, only the innovators win."[3] Responding to this directive and imperative, the Chinese People's Liberation Army (PLA) has been actively exploring a range of new theories, capabilities, and technologies that are believed to be critical to future operational advantage.[4] The PLA is looking to improve its capacity to leverage academic and commercial developments in the process through China's national strategy of "military-civil fusion" (军民融合).[5] In particular, Chinese innovation is poised to pursue synergies among brain science, artificial intelligence (AI), and biotechnology that may have far-reaching implications for its future military power and aggregate national competitiveness. Chinese military leaders appear to believe that such emerging technologies will be inevitably weaponized, often pointing to a quotation by Engels: "Once technological advancements can be used for military purposes and have been used for military purposes, they very immediately and almost necessarily, often violating the commander's will, cause changes or even transformations in the styles of warfare."[6] The PLA intends to achieve an operational advantage through seizing the initiative in the course of this transformation.

Chinese Military Innovation in the New Era

Chinese military scientists and strategists have often been animated in their thinking by concern with the progression of the ongoing revolution in military affairs (RMA) that is believed to be catalyzed by today's technological advancements.[7] The PLA has closely examined the U.S. military's approach to warfare, applying

Ms. Elsa B. Kania is an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security. Her views are her own.

lessons learned to its own military modernization in seeking to catch up, while also looking for opportunities to pursue asymmetric capabilities or attempt to achieve a first-mover advantage to overtake this "powerful adversary" (强敌). Since the 1990s, Chinese military modernization has particularly concentrated on pursuing a strategy of "informatization" (信息化).[8] Through this agenda, the PLA has developed an array of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems and concentrated on advancing capabilities for information operations (信息作战), including cyber warfare, electronic warfare, and psychological warfare.[9]

Today, PLA strategists anticipate a new style of warfare is on the horizon, as the character of conflict evolves from informatized toward "intelligentized" (智能化) warfare, in which AI, along with a range of technologies, is changing the form of warfare.[10] According to Lt. Gen. Liu Guozhi (刘国治), Director of the Central Military Commission Science and Technology Commission, "AI will accelerate the process of military transformation, ultimately leading to a profound Revolution in Military Affairs . . . The combination of artificial intelligence and human intelligence can achieve the optimum, and human-machine hybrid intelligence will be the highest form of future intelligence."[11] This striking statement highlights the PLA's interest at the highest levels in the notion of "hybrid intelligence" (混合智能), a concept that implies a blending of human and machine intelligence, including through leveraging insights from brain science and such techniques as the use of brain-computer interfaces.[12] This concept is not merely abstract but is starting to be realized through new programs, including projects intended to promote human performance enhancement. Future intelligentized operations (智能化作战) are expected to involve prominent employment of intelligent autonomy (智能自主) in weapons systems under conditions of multi-domain integration (多域一体) with command exercised through brain-machine integration, enabled by cloud infrastructure.[13] Chinese military scientists and strategists expect that this revolution in warfare will also demand transformation of the human element of warfare, which may require seeking command of the brain and biological sciences.

Reforming for Innovation

China's military reforms have elevated the importance of innovation in ways that could contribute to the PLA's ability to overcome prior difficulties. In this new era of Chinese military power, the PLA is seeking to reorient toward a model that leverages science and technology as core enablers of combat capabilities.[14] Pursuant to the reforms, the PLA has created the CMC Steering Committee on Military Scientific Research, which is responsible for establishing high-level priorities and strategic directions.[15] The CMC Science and Technology Commission (S&TC) has also been elevated to lead and guide military technological innovation and to promote military-civil fusion.[16] The S&TC oversees a number of plans, programs, and expert groups of top scientists for priorities that include human-machine fusion intelligence and biotechnology.[17] The CMC S&TC also has launched a plan and fund focused on cutting-edge technologies, and its "rapid response small group" on defense innovation is looking to help the PLA improve its capacity to leverage commercial technologies, including new techniques for human-machine interaction.[18]

China's military scientific enterprise has been transformed in the course of the PLA's reforms.[19] The PLA's Academy of Military Science (AMS), which has been responsible traditionally for issues of strategy and doctrine, has been officially designated to lead the PLA's military scientific enterprise.[20] AMS has launched the National Innovation Institute for Defense Technology (国防科技创新研究院),

which includes research institutes that focus on not only unmanned systems and artificial intelligence but also frontier/cutting-edge interdisciplinary (前沿交叉) technologies,[21] such as biotechnology and quantum technology.[22] The leadership of AMS also possesses the expertise and authority to promote these new directions in military innovation. Notably, Lt. Gen. Yang Xuejun (杨学军), who is known for his research in supercomputing and artificial intelligence, has become its President as of July 2017.[23] As Vice President, Maj. Gen. He Fuchu (贺福初), formerly President of the Academy of Military Medical Sciences (AMMS), is known for his research interests in genomics and bioinformatics, and he has also been prominent in emphasizing the importance of biotechnology as a new "strategic commanding heights" (制高点) of strategic competition.[24] Their selection to lead AMS appears to highlight the extent to which the PLA has prioritized these strategic technologies as a new direction for its development.

The PLA's paradigm for military innovation looks to promote integration of theory and technology to advance the development of new concepts and capabilities.[25] Notably, the CMC S&TC has been funding a program on biological interdisciplinary sciences and technology. This initiative includes projects on military brain science, advanced biomimetic systems, biological and biomimetic materials, and human enhancement.[26] In parallel with the China Brain Project, which has been launched as a national initiative for the 2016–30 timeframe, the CMC S&TC also appears to have launched a military brain science project that is exploring the potential of advances in neuroscience for military applications.[27] According to Hu Dewen (胡德文), a prominent researcher from the PLA's National University of Defense Technology (NUDT), the PLA should recognize the concurrent importance of and relationship among artificial intelligence, biological intelligence, and hybrid intelligence.[28]

PLA Expectations for Future Warfare

Chinese strategists anticipate that the tempo and complexity of operations will increase, perhaps dramatically, as the form (形态) or character of warfare continues to evolve.[29] As a result, PLA thinkers are concerned about the intense cognitive challenges that future commanders will encounter, particularly considering the importance of optimizing human-machine coordination (人机协同) and fusion or integration (人机融合).[30] Necessarily, these trends have intensified the PLA's interest in the military relevance of not only artificial intelligence but also brain science and new directions in biological interdisciplinary (生物交叉) technologies, ranging from biosensing and biomaterials to options for human enhancement.[31] The transition from informatization to intelligentization is seen as necessitating the upgrading of human cognitive performance to keep pace with the complexity of warfare.

In future conflict, the battlefield is expected to extend into new virtual domains. According to He Fuchu, "The sphere of operations will be expanded from the physical domain and the information domain to the domain of consciousness (意识域); the human brain will become a new combat space."[32] Consequently, success on the future battlefield will require achieving not only "biological dominance" (制生权) but also "mental/cognitive dominance" (制脑权) and "intelligence dominance" (制智权).[33] These nascent concepts, which are becoming more regularly discussed in influential writings, reflect the PLA's recognition of the increasing importance of contesting superiority within these new frontiers to achieving advantage.[34] Despite the complexity and capability of advanced technologies, this human element of warfare remains a critical vulnerability and source of potential advantage. At the same time, the notion of "winning without fighting" (不战而屈人之兵) is a traditional element of Chinese strategic thinking that possesses enduring relevance in an era

in which technology is becoming ever more consequential to strategic competition in peacetime.[35]

Human and Artificial Intelligence on the Future Battlefield

The PLA recognizes the advent of AI as a challenge and opportunity to seize the initiative in future military competition.[36] In fact, some military academics even anticipate that AI "will transcend firepower, machine power, and information power, becoming the most critical factor in determining the outcome of warfare."[37] In future "intelligentized operations," algorithmic advantage could become a dominant determinant of operational advantage, yet operations to subvert and counter an adversary's intelligentized capabilities ("逆智能化") are also seen as potentially advantageous, particularly for a weaker military.[38] Indeed, AI also possesses a number of limitations at present, including on issues of safety and security that may render it vulnerable to exploitation.

PLA scholars and strategists are continuing to debate the appropriate relationship between human and machine intelligence on the battlefield.[39] In an authoritative commentary, the CMC Joint Staff Department urged the PLA to take advantage of the "tremendous potential" of AI in operational command, planning and deductions, and decision support.[40] Whereas some scholars have warned against autonomous decisionmaking, other researchers have differentiated between the eventual necessity for automation or "intelligentization" of command decisionmaking at the tactical level of warfare, the importance of the delegation of command authorities in campaigns, and the imperative of human control in strategic decisionmaking, in which AI can take on a supporting function.[41] PLA thinkers recognize the importance of leveraging the relative strengths of human and machine intelligence respectively, and this interaction necessitates progress in techniques for human-machine coordination in combat.

These dynamics of future intelligentized operations elevate the criticality of cognition. A growing number of PLA scholars and strategists have argued that "mental/cognitive dominance" (制脑权) and "intelligence dominance" (制智权), concepts that are characterized as interrelated or sometimes synonymous in recent writings, will become the key points of struggle (制权争夺点).[42] Unlike traditional operations, the confrontation is occurring increasingly in the space of human intelligence (人的智力空间) and inherently involves "competition for cognitive speed and quality advantage," which can be enabled by data fusion.[43] The importance of speed, efficiency, and flexibility in intelligentized operations has provoked consideration of not only options for intelligent decision support systems,[44] but also "brain-machine fusion" (脑机融合) as a future paradigm for command and control, which would require integrating the art of command with emerging scientific and technological advancements.[45] The notion of brain control (脑控) primarily involves brain-machine/computer interface (脑–机接口) technology that is intended to enable efficient human-machine integration (人机融合), and PLA researchers continue to explore multiple modalities of human-machine interaction for command and control.[46] At the same time, cognitive enhancement, such as through the use of transcranial magnetic stimulation, could be leveraged to achieve an advantage in complex battlefield environments, in which there will be a high degree of integration between humans and weapons systems.[47]

PLA strategists believe that achieving "mental dominance" (制脑权) will be critical in future military competition across the spectrum from peacetime to warfighting.[48] Increasingly, this concept has recurred in PLA writings that emphasize the criticality of the "cognitive domain" (认知领域), which involves "the field of decision-making through reasoning," as the speed and complexity of conflict continue to increase.[49] Success in subverting

an adversary's cognition can enable "winning without fighting."[50] The increased integration of human cognition with technology influences military perception confrontation (军事感知对抗), which involves attempts to hinder and distort the adversary's cognition, whether through technical, physiological, or psychological techniques.[51] In an era of informatized warfare, conflict in the cognitive domain attempts to undermine the adversary's will and resolve, undermine perception and command capabilities to weaken fighting spirit, and manipulate decisionmaking.[52] The study of operations undertaken by the U.S. and Russian militaries has also influenced Chinese military thinking on the importance of psychological operations, but PLA thinkers are seeking to innovate their own tactics and concepts of operations,[53] including exploring the potential employment of intelligent agents to enable "guidance" of public opinion.[54] In particular, the prominence of social media and advances in artificial intelligence, including such techniques as deep fakes, have created new options for subversion and manipulation. The PLA is actively pursuing research and the development of capabilities, which could range from the use of the drug Modafinil for performance enhancement, to leveraging insights from brain science and psychology to target and exploit inherent vulnerabilities in human cognition. While apparently enthusiastic about the offensive potential of such options, the PLA is concerned about the potential for subversion of its own forces, including persistent anxieties about the prospects of color revolution.[55]

Consequently, the pursuit of advances in military brain science is recognized as important to advancing future battlefield effectiveness.[56] In particular, this new domain in military competition is seen as variously involving attempts to "imitate the brain" (仿脑), leverage "brain control" (脑控), "enhance the brain" (超脑), or "control the brain" ("控脑").[57] On the battlefield, attempts to undermine an adversary could include interfering with the adversary's capacity for cognition, whether through manipulation or outright destruction, from disrupting the flow of data to exploiting ideology or emotion.[58] Increasingly, "mental confrontation" (脑对抗) could become a major feature of future conflicts, involving attack, defense, and enhancement of the brain.[59] Maj. Gen. He Fuchu has anticipated the development of "a new brain-control weaponry" that interferes with and controls people's consciousness, thereby subverting combat styles.[60] Concretely, Zhou Jin (周瑾), a researcher with the Institute of Military Cognition and Brain Science at AMMS, has concentrated on brain science and neural engineering, and his research has also contributed to an expert group on psychological warfare and cognitive technology through the CMC Science and Technology Commission.[61]

The PLA's intended integration of human and machine intelligence could be eventually facilitated by advances in brain-machine interfaces. For instance, at the PLA's National University of Defense Technology (NUDT), the Cognitive Science Basic Research Team (认知科学基础研究团队) has been engaged in research on brain-machine interfaces (脑机接口) for more than 20 years, such that this technology can now be used to operate a robot, drive a vehicle, or even to operate a computer, enabled by the processing of EEG signals.[62] "Combining the high functioning of the machine with the high intelligence of human beings to achieve high performance of equipment systems, this is an important domain of application in intelligent science," according to Hu Dewen (胡德文), who has led this program.[63] In the PLA's Information Engineering University's Information Systems Engineering College, Tong Li (通李) has been engaged in research on intelligent information processing and brain-computer interaction (脑机交互), which has been reportedly leveraged to enable brain control of a drone or robot.[64] Meanwhile, at AMMS, Wang Changyong (王常勇), Deputy Director of the

Institute of Military Cognition and Brain Science, has engaged in research on brain-machine interfaces, variously pursuing EEGs (via the scalp) and implants in the cranial nerves of macaques, which are believed to be an apt model to simulate human cognition, concentrating on neural information acquisition.[65] The complexity of these challenges are seen as increasing the importance of sophisticated simulations in combat laboratories that can explore the efficacy of these human-machine synergies.[66]

In advancing these techniques, the PLA could leverage academic research and commercial developments. For instance, Tsinghua University, which is actively supporting military-civil fusion, has been pursuing research on human-machine interaction (人机协作) with funding from the CMC Science and Technology Commission.[67] In Tianjin, a local action plan has called for research in brain-computer interface technologies, including brain-controlled unmanned systems and even automatic sniper rifles.[68] At Tianjin University, the Academy of Military Science and the Chinese Academy of Launch Vehicle Technology have both established joint laboratories and partnerships that concentrate on innovation in human-machine hybrid intelligence (人机混合智能).[69] The State Key Laboratory of Cognitive Science and Learning, based at Beijing Normal University, has also pursued initiatives in military-civil fusion.[70]

Pursuant to military-civil fusion, Chinese advances in brain-computer interface research undertaken by academic institutions or commercial enterprises may eventually have military relevance. During the past couple of years, the Chinese government has convened a national competition on brain-computer interfaces, of which the PLA NUDT is a co-sponsor.[71] In addition, AMMS researchers have engaged with a commercial enterprise that is specializing in the development of EEG products, known as Cogrowth (*ku chengzhang*, 酷成长), which has concentrated in its products on brain-computer interface and intelligent control with applications that include attention and memory training.[72] Meanwhile, Tianjin University and the China Electronics Corporation have achieved new breakthroughs in research on a brain-computer interface (BCI) chip, known as "Brain Talker," which is specially designed to decode brainwave information.[73] The advantages of this chip are described as including its size, precision, efficiency in decoding information, and increased capability for fast communication, all of which can contribute to the realization of BCI technologies.[74] According to its designers, "this BC3 (Brain-Computer Codec Chip) has the ability to discriminate minor neural electrical signals and decode their information efficiently, which can greatly enhance the speed and accuracy of brain-computer interfaces."[75] So too, as combat platforms are expected to progress from "informatization" to "low intelligentization" to "brain-like high intelligentization," such breakthroughs in brain-like computing chips are anticipated to be important to advancing autonomy.[76]

As the cognitive demands for commanders are expected to become more acute on the future battlefield, new directions in integrating human and machine intelligence could prove militarily advantageous. Through leveraging "brain networking" (脑联网), a "combat brain" (作战大脑) can be developed for the future battlefield, which is expected to enhance the cognitive and decisionmaking capabilities of military commanders, including through improving their cognitive capability and understanding of the battlefield situation, according to NUDT scholars.[77] Hypothetically, a so-called "network of brains" could accelerate real-time transmission of data on the battlefield, based on leveraging brain-machine interfaces to facilitate communication between commanders and their units. Wu Haitao (吴海涛), a researcher with AMMS, has postulated;

> *"Brain networking" technologies are far from mature, but we have good reason to*

> *believe that bio-intelligence networks based on brain intelligence will inevitably surpass existing informatized technology and weak artificial intelligence technologies. The development and application of related technologies will inevitably accelerate disruptive transformations in the military domain. In the future, a brain-to-brain collaborative combat platform or system based on "brain networks" may be exploited, which can be expected to achieve high-level optimization and integration of battlefield perception, logistics support, weaponry and command systems, maximize combat links and command effectiveness, so as to capture fleeting opportunities in the ever-changing battlefield situation and achieve unexpected victories.*[78]

The notion of brain networking through brain-to-brain interfacing may sound fanciful, but there are initial experimental indications that this could become a technical possibility. For instance, in an experiment at Zhejiang University, researchers created a so-called rat cyborg through implanting microelectrodes into the brain of a live rat, which connected it to the brain of a human "manipulator" who had been connected to a computer brain-machine interface, by which the rat was directed to navigate a maze.[79]

The future trajectory of such advances could be shaped by the continued implementation of the China Brain Project, which was launched in 2016.[80] The project, which was initially initiated in response to the U.S. brain science program, is recognized as a megaproject for the 2016–2030 timeframe.[81] It may receive billions in funding once fully realized.[82] The leading researcher involved in the design of this project, Mu-Ming Pu of the Chinese Academy of Sciences, has described this project as involving "two wings," encompassing not only brain science but the intersection between brain science and artificial intelligence, which is believed to be highly promising.[83] The focus on imitation of the brain often involves brain-like and brain-inspired intelligence, which is a high-level priority highlighted in China's New Generation Artificial Intelligence Development Plan and operationalized through a new national laboratory dedicated to the topic.[84] In addition, in September 2015, Beijing's Science and Technology Commission announced the launch of a special project on brain science research to concentrate on brain cognition, brain medicine, and brain-like computing. This center plans to support projects that leverage new biomedical techniques, including high-throughput single-gene sequencing and precise genome editing, enabled by big-data processing.[85] The involvement of AMMS is notable but hardly surprising considering that neuroscience has been highlighted as a priority in China's plans for military-civil fusion, and there may be interesting synergies between academic research and potential military applications.[86]

This research agenda is starting to translate into practical advances. For instance, the Tianjic chip leverages a brain-inspired architecture, and its designers claim that it represents an important progression toward artificial general intelligence that is comparable to humans in its capabilities.[87] As one prominent academic highlighted, "Human beings have gradually entered the era of artificial intelligence, but the understanding of the essence of what constitutes 'intelligence' remains unclear. The study of brain and cognition will promote people's understanding of the essence of 'intelligence' and promote the development of related technologies and industries."[88] Seemingly speculatively, these attempts at imitating human cognition have been described as possessing the potential to extend to the development of highly intelligent weapons systems capable of reasoning and judgment comparable to that of a human.[89]

Within the same timeframe, the CMC S&TC has also launched a military brain science plan and

projects that appear to be occurring in parallel—and perhaps with some degree of integration or coordination—with China's national brain science project.[90] For instance, Wu Shengxi (武胜昔), a professor with the Fourth Military Medical University who is engaged in both initiatives, has concentrated his research on the plasticity of the central nervous circuits and mechanisms of advanced brain function.[91] His activities have included collaboration with a senior scientist from MIT's Broad Institute and the McGovern Institute for a project on the anterior cingulate cortex, a region of the brain that "plays a role in fundamental cognitive processes, including cost-benefit calculation, motivation, and decisionmaking."[92] Chinese academic and military medical institutions have concentrated on the expansion of military brain science, which has been prioritized for support and funding.[93] Overall, the discipline of military cognitive neuroscience continues to evolve and involves several interrelated research directions, which can include brain monitoring (for example, to measure and assess the military mental work); brain modulation (mind-controlling targets and effects); brain damage; and brain promotion (neuro-scientific training methods).[94] For instance, the first seminar convened on brain science research and military-civil fusion collaborative innovation concentrated on core competencies of battlefield perception, command and control, target striking, identifying ten key research directions for such military cognitive capabilities (军事认知能力).[95]

Chinese research is anticipated to have certain potential advantages in this field. China's rapidly aging population presents an acute societal challenge but also an opportunity to leverage sizable amounts of data about brain disease.[96] At the same time, the prevalence of primate research in China could prove another significant advantage. At a time when the United States and Europe have started to cut back on primate research due to

Game-changing synthetic biology research may enable future capabilities for Soldiers (U.S. Army Photo by Eric Proctor and Autumn Kulaga)

ethical concerns and expense, these programs have continued to expand in China with robust state support.[97] The Chinese government has undertaken significant investments to expand its own neuroscience research with non-human primates, which are believed to be "ideal animal models for understanding human brain and cognition."[98] In particular, China has become a global center for research involving macaque monkeys, which are seen as well-suited as a model for research on the human brain.[99] In one notable study, researchers introduced the MCPH1 gene, which is believed to be linked to brain development, into embryos to create transgenic macaque monkeys that demonstrated improved performance on short-term memory tasks, while also displaying a longer process of brain development, such as that characteristic of humans.[100] This study was described as "the first attempt to experimentally interrogate the genetic basis of human brain origin using transgenic monkey models.[101] Similarly, in another greatly controversial undertaking, researchers have been creating embryos that represent "human-animal chimeras"—in this case, monkey embryos to which human cells are added.[102] These changes in the Shank3 gene are expected to cause mutations in the brains of monkeys that have been

edited.[103] The use of gene editing to improve models for studying the brain illustrates the important intersections between cognitive science and biotechnology, which has emerged as a parallel emphasis for the PLA.[104]

Biotechnology on the Future Battlefield

The PLA's keen interest in the impact of biology on military affairs is also reflected in strategic writings and research that argue today's advances in biology are contributing to an ongoing evolution in the form or character (形态) of conflict.[105] In one prominent example, Guo Jiwei (郭继卫), a professor with the Third Military Medical University, wrote *War for Biological Dominance* (制生权战争), published in 2010, highlighting the multifaceted applications of biology in future warfare.[106] PLA researchers with the Academy of Military Medical Sciences have highlighted that advances in science and technology drive evolution in the character of conflict, raising the concept of "biology-enabled" warfare (生物化战争).[107] The PLA also sees synthetic biology as a domain with great military potential.[108] Unsurprisingly, the PLA has been concerned with advances in biotechnology in the United States and worldwide, particularly the Defense Advanced Research Projects Agency's launch of the Biological Technologies Office. The Chinese government has highlighted biotechnology as an industry that promises major commercial advantages, and China's plans and initiatives for military-civil fusion have prioritized biology as a critical sector.[109] Beyond outright military research, there is an emerging ecosystem of academic and commercial enterprises that is or could become involved in supporting military research.

Increasingly, the PLA is starting to recognize biology as a new domain of warfare and elevating its importance in strategic thinking. The concept of biological dominance (制生权) could be rendered as "command and superiority in biology," and PLA scientists and scholars are continuing to work toward developing more cohesive theories around these ideas that could contribute to future concepts of operations.[110] In the new RMA, biotechnology will become the new "strategic commanding heights," declared He Fuchu, then president of the Academy of Military Medical Sciences, in 2015.[111] He has remained a prominent advocate for the militarization of biotechnology. Since 2016, Maj. Gen. He has also been appointed to serve on the CMC S&TC, which promotes military-civil fusion and technological innovation, where he may be involved in guiding research on biology and interdisciplinary technologies, from biomimetic and biomaterials to biosensing technology, that could contribute to future advances in weaponry.[112] He has predicted, "As the weaponization of living organisms will become a reality in the future, non-traditional combat styles will be staged, and the 'biological frontier' (生物疆域) will become a new frontier for national defense."[113] He goes on to say that;

> *Biological interdisciplinary technology will make future combat platforms move toward human-computer integration and intelligentization. In the future, human-like brain information processing systems will achieve revolutionary breakthroughs, such as high-performance low-power computing, highly intelligent autonomous decision-making, active learning, and continuous increases in intelligentization, promoting the emergence of highly intelligentized and autonomous combat forces.*[114]

Certain elements of PLA strategic thinking on the offensive potential of these technologies are troubling. Notably, the 2017 edition of *Science of Military Strategy* (战略学), a textbook published by the National Defense University that is typically considered relatively authoritative, introduced a new section dedicated to the topic of military struggle

in the domain of biology. While this book does not mention CRISPR specifically, it notes that new kinds of biological warfare could be targeted, employing "specific ethnic genetic attacks" (特定种族基因攻击). Disturbingly, the discussion of this possibility is repeated across a number of PLA writings.[115] Indeed, "biological deterrence" (生物威慑) should be considered a new kind of deterrence that is enabled by advances in biotechnology, including the potential for "ethnic-specific genetic weapons" ("种族特异性基因武器"), according to Zeng Huafeng (曾华锋) of the PLA's NUDT.[116] "Due to the high lethality, low cost and diverse means of genetic attack, it will have a profound impact on future wars" in ways that could increase the destructiveness of warfare, according to NUDT researcher Shi Haiming (石海明).[117] As a result, the outcome of war may no longer determined by the destruction of combat, but rather there could be further blurring of the boundaries between peace and warfare.[118] These relatively authoritative discussions of the potential for genetic attacks remain ambiguous but are troubling nonetheless, given the emergence of technologies that create new possibilities in gene editing.[119]

To date, China has been leading in early trials of CRISPR in not only animals but also human patients.[120] The emergence of Chinese research as a new frontier for experimentation with CRISPR reflects factors that include lesser regulatory requirements and robust support and enthusiasm for leveraging these technologies. To date, CRISPR research in China has concentrated heavily on applications in agriculture and for medical or therapeutic purposes.[121] It is also striking that a significant proportion of the research in CRISPR is occurring at Chinese military medical and research institutions, especially the PLA General Hospital.[122] The centrality of PLA institutions in this CRISPR research is concerning when juxtaposed with known programs and indications of military interest in human enhancement. In one notable example, a student at the Academy of Military Medical Science wrote a doctoral dissertation in 2016 titled "Research on the Evaluation of Human Performance Enhancement Technology."[123] This dissertation pointed to CRISPR-CAS as one of three primary "human performance enhancement technologies" (人效能增强技术) that can be employed to increase the combat effectiveness of military personnel.[124] The researcher dissertation highlights that CRISPR holds "great potential" as a "disruptive" technology, arguing that therefore China must "grasp the initiative." Although the practical application for performance enhancement appears to remain a more distant possibility at this point, such research provides at the very least indication of interest and concern.

Although the use of CRISPR as a technique for gene editing remains novel and nascent, these tools and techniques are rapidly advancing, and what is within the realm of the possible for military applications may continue to shift as well. In the meantime, throughout China, gene editing is already under way in animals, human embryos, and even in clinical trials. In the process, BGI, formerly known as Beijing Genomics Inc., has been very active in CRISPR research.[125] BGI has also provoked controversy after attempting to commercialize genetic editing of animals, such as mini-pigs as pets, and from pursuing research on the genetic basis of intelligence by soliciting DNA from geniuses.[126] Of course, gene editing today remains constrained by persistent difficulties, such as the issue of limiting off-target effects, which can cause unintended consequences in the genome.[127] However, current research has continued to work toward making gene editing more precise and practical, and BGI has established an edge in cheap gene sequencing, concentrating on amassing massive amounts of data from a diverse array of sources.[128] BGI has achieved a global presence, including laboratories in California and Australia, and its activities have continued to expand.[129]

The Chinese government clearly believes that national genetic resources possess strategic significance. China's National Genebank, which is administered by BGI, was launched in 2016, and it is intended to become the world's largest. By some accounts, its establishment was motivated at least partly by issues of biosecurity, particularly that of Chinese genomic information then being stored in overseas facilities.[130] This new Chinese genebank has been described as intended to "develop and utilize China's valuable genetic resources, safeguard national security in bioinformatics, and enhance China's capability to seize the strategic commanding heights" in the domain of biotechnology. These concerns about the potential strategic significance of genetic resources have also resulted in an unwillingness to share and exchange data, even as Chinese companies are avidly seeking out access to sources of data beyond China.[131]

The processing of such massive amounts of genetic information requires powerful supercomputers. In the process, BGI affiliates have been engaged in research collaboration with the NUDT, including the development of tools and insights that may contribute to enabling future gene editing.[132] In particular, one former professor who remains affiliated with the NUDT has also maintained a position with BGI as a specially appointed professor.[133] Their research concentrates on bioinformatics, leveraging supercomputers, namely the Tianhe, for the processing of genetic information in biomedical applications.[134] Such collaboration with NUDT researchers is not necessarily surprising.[135] However, such confluence of troubling sentiments in military writings, ongoing programs funding research on human enhancement, and collaboration between military and commercial institutions raises questions that merit further scrutiny from a policy perspective, particularly considering the range of potential implications of BGI's research.[136]

Looking forward, the application of machine learning to the analysis of genomic information could enable the discovery of patterns and insights that may prove actionable. China has also been at the forefront of parallel progress in precision medicine that is enabled by the embrace of AI for medical applications. In the field of AI, China has been sometimes characterized as possessing an advantage in data. However, the actual impact of data depends on context, techniques, and intended applications. It seems more likely that China could possess and achieve a data advantage in genomics and biomedical technologies, based on the sizable amounts of genomic and medical data that have been and continue to be collected. This access to genomic information combined with continued advances in artificial intelligence could contribute to advances in understanding of the evolution of the human brain and genomic determinants of intelligence.[137] So too, the study of the human genome and its comparison with that of other primates can contribute to identifying which specific genomic differences account for the uniqueness of the human brain. Potentially, such insights can also enable future augmentation of human intelligence in ways that enable the "mental dominance" and superiority in intelligentized operations that the PLA believes is essential to success in future warfare.

Conclusions and Implications

Although technological advantage has been a key pillar of U.S. military power and national competitiveness, China is catching up, aspiring to take the lead in today's strategic technologies. Pursuing military innovation as a priority and national imperative, the Chinese military appears to be enthused with the possibility that today's RMA could disrupt the future military balance to its advantage. Today, China possesses a stronger technological foundation for future military power, despite confronting continued challenges in the development of "key

and core" (关键核心) technologies, and the PLA is looking to improve its capacity to leverage academic and commercial advancements to enable future military capabilities, including artificial intelligence, biotechnology, and quantum technology.

The PLA is greatly concerned about being subject to technological surprise and equally concerned with opportunities to achieve it. Future primacy in these fields, which could prove important to future military advantage, may remain highly contested between the United States and China. However, the process of military innovation that is required to operationalize these capabilities will prove inherently challenging, and the feasibility of certain aspects of the PLA's strategic thinking and theoretical explorations remains to be seen. Of course, these technologies remain quite nascent, and the process of research, development, experimentation, and operationalization that is required to realize their full potential may be lengthy and complex, requiring adjustments that are challenging for any bureaucracy.

However, the PLA today is fighting to innovate. It is striking that the PLA has introduced major changes and reforms to its military scientific enterprise, including through efforts to recruit and support more junior scientists, while also recruiting more civilians for technical positions. The prominence of military scientists in PLA leadership may also provide powerful champions for this agenda. Ultimately, Xi Jinping's demand that the PLA pursue innovation could serve as a powerful impetus for peacetime innovation, even as the ideological constraints upon an authoritarian military that is de facto the armed wing of the Chinese Communist Party could impede creativity and initiative. The future trajectory of these concepts and potential capabilities will merit continued analytic and academic attention as such research progresses. PRISM

Notes

[1] "The CCP Central Committee and State Council Release the 'National Innovation-Driven Development Strategy Outline'" [中共中央 国务院印发《国家创新驱动发展战略纲要], *Xinhua*, May 19, 2016, available at <http://news.xinhuanet.com/politics/2016-05/19/c_1118898033.htm>. See also Xi Jinping's remarks on this approach in the context of military modernization: "Xi Jinping: Comprehensively Advance an Innovation-Driven Development Strategy; Promote New Leapfrogging in National Defense and Military Construction" [习近平：全面实施创新驱动发展战略 推动国防和军队建设实现新跨越], *Xinhua*, March 13, 2016, available at <http://news.Xinhuanet.com/politics/2016lh/2016-03/13/c_1118316426.htm>.

[2] "Xi Jinping: Accurately Grasp the New Trends in Global Military Developments and Keep Pace with the Times, Strongly Advancing Military Innovation" [习近平：准确把握世界军事发展新趋势 与时俱进大力推进军事创新], *Xinhua*, August 30, 2014, available at <http://news.xinhuanet.com/politics/2014-08/30/c_1112294869.htm>.

[3] See, for instance Xi Jinping's remarks as quoted in this article: "Scientific and Technological Innovation, A Powerful Engine for the World-Class Military" [科技创新，迈向世界一流军队的强大引擎], *Xinhua*, September 15, 2017, available at <http://www.gov.cn/xinwen/2017-09/15/content_5225216.htm>.

[4] "The CCP Central Committee and State Council Release the 'National Innovation-Driven Development Strategy Outline.'"

[5] "Xi Jinping's Talk on Military-Civil Fusion: Regarding the Whole Outlook for National Security and Development" [习近平谈军民融合：关乎国家安全和发展全局], *Seeking Truth* [求是], October 16, 2018, available at <http://www.qstheory.cn/zhuanqu/rdjj/2018-10/16/c_1123565364.htm>.

[6] Cai Yubin [蔡渭滨] and Huang Xuebin [黄雪斌], "Vigorously Cultivate the Fighting Spirit of Scientific and Technological Personnel" [大力培育科技人员的战斗精神], *PLA Daily*, May 6, 2019, available at <http://www.xinhuanet.com/mil/2019-05/06/c_1210126997.htm>.

[7] "Xi Jinping: Accurately Grasp the New Trend in Global Military Developments."

[8] For an earlier perspective on this RMS, see Jacqueline Newmyer, "The Revolution in Military Affairs with Chinese Characteristics," *The Journal of Strategic Studies* 33, no. 4 (2010): 483–504; You Ji, "Learning and Catching Up: China's Revolution in Military Affairs Initiative," in *The Information Revolution in Military Affairs in Asia* (New York: Palgrave Macmillan, 2004), 97–123; Andrew S. Erickson and Michael S. Chase, "Informatization and the Chinese People's Liberation

Army Navy," in *The Chinese Navy: Expanding Capabilities, Evolving Roles*, ed. Phillip Saunders et al. (Washington, DC: National Defense University Press, 2011): 247–287.

[9] Ye Zheng [叶证], *Lectures on the Science of Information Operations* [信息作战科学教程] (Beijing: Military Science Press [军事科学出版社], 2013).

[10] "Xi Jinping's Report at the Chinese Communist Party 19th National Congress" [习近平在中国共产党第十九次全国代表大会上的报告]; "Experts: Military Intelligentization Is Not Merely Artificial Intelligence" [专家：军事智能化绝不仅仅是人工智能], *People's Daily*, December 6, 2017, available at <http://military.people.com.cn/n1/2017/1206/c1011-29689750.htm>.

[11] "Lt. Gen. Liu Guozhi: The Development of Military Intelligentization Is a Strategic Opportunity for our Military to Turn Sharply to Surpass" [刘国治中将:军事智能化发展是我军弯道超车的战略机遇], CCTV News, October 22, 2017, available at <http://mil.news.sina.com.cn/china/2017-10-22/doc-ifymzqpq3312566.shtml>.

[12] Ibid.

[13] "Setting off a new revolution in military affairs? Six key words to interpret intelligentized operations" [掀起新的军事革命？六大关键词解读智能化作战], *PLA Daily*, March 1, 2018, available at <http://www.xinhuanet.com/mil/2018-03/01/c_129819887.htm>

[14] See the latest defense white paper that provides an official discussion of the reforms: "China's National Defense in a New Era," *Xinhua*, July 24, 2019, available at <http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm>.

[15] Ibid.

[16] Ibid.

[17] There are further details available upon request. There are multiple references to this program in publicly available information.

[18] "The whole country's first national defense scientific and technological innovation rapid response small group launched in Shenzhen" [全国首个国防科技创新快速响应小组在深圳启动], Shenzhen Special Zone Daily [深圳特区报], available at March 18, 2018, <http://news.sina.com.cn/c/nd/2018-03-18/doc-ifyskmpr7659375.shtml>

[19] "Xi Jinping: Strive to Build a High-level Military Scientific Research Institution to Provide Strong Support for the Party's Strong Military Objective in the New Era" [习近平：努力建设高水平军事科研机构 为实现党在新时代的强军目标提供有力支撑], *Xinhua*, May 16, 2018, available at <http://www.xinhuanet.com/2018-05/16/c_1122843283.htm>.

[20] "China's National Defense in the New Era."

[21] "Frontier" is my chosen rendering of *qianyan* (前沿), which can also be rendered as "frontline," "forward position," "cutting-edge," or "advanced."

[22] "Academy of Military Science National Defense Science and Technology Innovation Research Academy—Exploring the "Matrix" Research Model to Enhance Innovation Capability" [军事科学院国防科技创新研究院—— 探索 "矩阵式" 科研模式提升创新能力], April 2, 2018, available at <http://www.81.cn/jfjbmap/content/2018-04/02/content_202957.htm>. See also "Academy of Military Science National Defense Science and Technology Innovation Research Academy Has Taken Measures to Gather Top Talents" [军科院国防科技创新研究院多措并集聚顶尖人才], *China Military Network*, February 4, 2018, available at <http://webcache.googleusercontent.com/search?q=cache:WDwIAWm-c6agJ:www.81.cn/jwgz/2018-02/04/content_7931564.htm+&cd=8&hl=en&ct=clnk&gl=us>.

[23] Yang Xuejun was the former commandant of the National University of Defense Technology, and transfer to lead AMS may reflect an elevation of AMS over NUDT.

[24] This shift could indicate a closer integration of medical science with military science. He Fuchu [贺福初], "The Future Direction of the New Global Revolution in Military Affairs" [世界新军事革命未来走向], *Reference News* [参考消息], August 24, 2017, available at <https://web.archive.org/web/20190823210313/http://www.xinhuanet.com/politics/2017-08/24/c_129687890.htm>.

[25] "'Theory-Technology Fusion Innovation' New Year Seminar Successfully Convened in Beijing" ["理技融合创新" 新春座谈会在京成功召开], China Association for Artificial Intelligence [中国人工智能学会], available at <https://web.archive.org/web/20191011035737/http://caai.cn/index.php?s=/Home/Article/detail/id/490.html>.

[26] The CMC S&TC's expert group on biology and cross-domain science and technology appears to guide these projects, involving scientists with expertise in neuroscience and biomaterials. The chief scientist of the expert group on this topic has also highlighted the military potential of technologies that include biosensing, biomimetic information processing, and biocomputing to enable new-type weapons and equipment.

[27] Mu-ming Poo et al., "China Brain Project: Basic Neuroscience, Brain Diseases, and Brain-Inspired Computing," *Neuron* 92, no. 3 (2016): 591–596.

[28] Hu Dewen, "Military School Scratches 'Cool Smart Wind'" [军校刮起 "炫酷智能风"], *PLA Daily*, July 19, 2019, available at <http://military.workercn.cn/32820/201907/19/190719101538199.shtml>. Hu Dewen has also received funding through National Key R&D Plan to pursue research on human-robot intelligent fusion technology. His research has included the use of neural networks in adaptive control.

[29] Chen Hanghui [陈航辉], "Artificial Intelligence:

Disruptively Changing the Rules of the Game" [人工智能：颠覆性改变"游戏规则], China Military Online, March 18, 2016, available at <http://www.81.cn/jskj/2016-03/18/content_6966873_2.htm>.

[30] See, for instance, "Experts: Military Intelligentization Is Not Merely Artificial Intelligence" [专家：军事智能化绝不仅仅是人工智能], *People's Daily*, December 6, 2017, available at <http://military.people.com.cn/n1/2017/1206/c1011-29689750.html>.

[31] These directions in the Chinese military's strategic thinking are assessed to be relatively authoritative based on the numerous articles and statements from high-level military scientists and strategists. Certain Chinese military scholars and scientists, including those affiliated with the Academy of Military Science and National University of Defense Technology, as well as several military medical institutions, have articulated these lines of argument across a range of books and articles that date back nearly a decade. However, these theories and concepts are unlikely to constitute official elements of doctrine at present.

[32] He Fuchu, "The Future Direction of the New Global Revolution in Military Affairs."

[33] Ibid.

[34] Often, the PLA starts to explore a high-level concept for which the meeting continues to evolve over time. At present, there is no official or doctrinal definition for these concepts, but I understand them as each referring to attempts to achieve an advantage in the domains of cognition, biology, and intelligence on the battlefield and in overall military competition. Often, such concepts originate the work in a prominent researcher but then become the subject of more general debate and might be eventually introduced into official planning and/or doctrinal materials.

[35] For one perspective on the issues, see Dean Cheng, "Winning without Fighting: The Chinese Psychological Warfare Challenge," *Science* 4 (2003): 30.

[36] *The Science of (Military) Strategy* released in 2017 by the PLA's National Defense University has added a new section on "military competition in the domain of (artificial) intelligence" (智能领域军事竞争), in an unusual, off-cycle revision of this authoritative textbook, of which Lt. Gen. Xiao Tianliang (肖天亮), who remains the vice commandant of the PLA's National Defense University, is the editor.

[37] Yun Guangrong [游光荣], "AI Will Deeply Change the Face of Warfare" [人工智能将深刻改变战争面], *PLA Daily*, October 17, 2018, available at <http://www.81.cn/jfjbmap/content/2018-10/17/content_218050.htm>.

[38] Li Minghai (李明海), "Where Is the Winning Mechanism of Intelligent Warfare?" [智能化战争的制胜机理变在哪里?], January 13, 2019, available at <http://webcache.googleusercontent.com/search?q=cache:2HxhOYXd2p0J:www.sohu.com/a/288730322_778557+&cd=2&hl=en&ct=-clnk&gl=us>. Li Minghai is a researcher with the PLA's National University of Defense Technology. Chen Yongyi [陈永义], "Focus on Confronting 'Counter-intelligentization' Operations" [重视应对"逆智能化"作战], *PLA Daily*, August 1, 2019, available at <http://www.81.cn/bqtd/2019-08/01/content_9575539.htm>.

[39] Yuan Yi [袁艺], Gao Dongming [高冬明], and Zhang Yujun [张玉军], "Also Discussing Intelligentized Command 'Autonomous Decision-Making'" [也谈智能化指挥"自主决策"], *PLA Daily*, April 18, 2019, available at <http://www.81.cn/jfjbmap/content/2019-04/18/content_231979.htm>.

[40] CMC Joint Staff Department [中央军委联合参谋部], "Accelerate the Construction of a Joint Operations Command System with Our Military's Characteristics" [加快构建具有我军特色的联合作战指挥体系], *Seeking Truth*, August 15, 2016, available at <http://www.qstheory.cn/dukan/qs/2016-08/15/c_1119374690.htm.

[41] Yuan, Gao, and Zhang, "Also Discussing Intelligentized Command 'Autonomous Decision-Making.'"

[42] Shen Shoulin [沈寿林] and Zhang Guoning [张国宁], "Understanding Intelligentized Operations" [认识智能化作战], *PLA Daily*, March 1, 2018, available at <http://www.81.cn/jfjbmap/content/2018-03/01/content_200671.htm>.

[43] Ibid; "Academician He You: Accelerate the Development of Maritime Information Processing Technology, and Provide Scientific and Technological Support for a Powerful Maritime Nation" [何友院士：加快发展海洋信息处理技术，为海洋强国提供科技支撑], *S&T Herald* [科技导报], November 2017, available at <http://www.cnki.com.cn/Article/CJFDTotal-KJDB201720001.htm, available in full text: https://web.archive.org/web/20191011051014/http://blog.sciencenet.cn/blog-336909-1084316.html>.

[44] Zhang Xiao-hai [张晓海] and Cao Xin-wen [操新文], "Military Intelligent Decision Support Systems Based on Deep Learning" [基于深度学习的军事智能决策支持系统], *Command Control & Simulation* [指挥控制与仿真] 40, no. 2 (April 2018). The PLA has been inspired by AlphaGo and AlphaZero in exploring such options, and an initial proof of concept has been demonstrated through "Prophet 1.0" (先知V1), an AI system developed by the Chinese Academy of Sciences Institute of Automation that was used in wargaming.

[45] Ibid.; "Academy of Military Medical Sciences Researcher Wu Haitao Explains to You 'What Will Brain Science Bring from the Military'" [军事科学院军事医学

研究院研究员吴海涛为您讲述——脑科学“从军”会带来什么?], available at <http://www.81.cn/jfjbmap/content/2019-04/26/content_232600.htm>.

[46] Chen Jian-hua [陈建华] et al., “Multi-modal Interaction Technology of Military Command and Control System” [军事指控系统多通道人机交互技术], *Command Control & Simulation* [指挥控制与仿真] 41, no. 4 (August 2019).

[47] For context, see Amanda M. Kelley et al., “Cognition Enhancement by Modafinil: A Meta-analysis,” *Aviation, Space, and Environmental Medicine* 83, no. 7 (2012): 685–690; Wang Shizhong [王世忠] and Hao Zhengjiang [郝政疆], “Brain Confrontation: Achieving a High Degree of Integration between Humans and Weapons” [脑对抗：人与武器实现高度融合], available at <https://web.archive.org/web/20190903022447/http://www.81.cn/jfjbmap/content/2019-01/25/content_226145.htm>.

[48] There are several potential alternative translations to zhinaoquan, including “mind/mental dominance,” “mind/mental superiority,” and “cognitive superiority.” The concept alludes to the superiority in reasoning and decisionmaking that is required to succeed on the battlefield. For the book that coined this term most prominently, see Zeng Huafeng [曾华锋] and Shi Haiming [石海明], *Mental Dominance: The Laws of War in the Global Media Age and National Security Strategy* [制脑权：全球媒体时代的战争法则与国家安全战略] (Beijing: People’s Liberation Army Press, 2014). See also: Nathan Beauchamp-Mustafaga, “Cognitive Domain Operations: The PLA’s New Holistic Concept for Influence Operations,” *China Brief* 19, no. 16, available at <https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/>.

[49] Zhu Xueling [朱雪玲] and Zeng Huafeng [曾华锋], “Mental Control Operations: New Model of Future Wars” [“制脑作战：未来战争竞争新模式”], *PLA Daily*, October 17, 2017, available at <https://web.archive.org/web/20191011053447/http://www.81.cn/jfjbmap/content/2017-10/17/content_189879.htm>; Luo Yuzhen [罗语嫣] et al., “The Common Domain Characteristics of Cognitive Domain and Its Key Techniques” [认知域的公域特性及其关键技术], *National Defense Science & Technology* [国防科技] 39, no. 4 (2018).

[50] Zhu and Zeng, “Mental Control Operations: New Model of Future Wars.”

[51] “Setting off a new revolution in military affairs? Six key words to interpret intelligentized operations” [掀起新的军事革命？六大关键词解读智能化作战], *PLA Daily*, March 1, 2018, available at <http://www.xinhuanet.com/mil/2018-03/01/c_129819887.htm>

[52] Wang Zhaowen [王照稳] and Fu Minghua [付明华], “Analysis of Cognitive Domain Warfare in Informatized Warfare” [信息化战争认知域作战探析], *PLA Daily*, July 28, 2015, available at <http://www.81.cn/jmywyl/2015-07/28/content_6602887.htm>; Shi Haiming [石海明] and Zeng Huafeng [曾华锋], “National Cognitive Space Security Strategy from the Perspective of Science and Technology and War” [科技与战争视角下的国家认知空间安全战略], *National Defense Science and Technology* [国防科技], no. 3 (2014), available at <http://www.cqvip.com/qk/96765a/201403/661703248.html>. The authors are affiliated with the PLA’s National University of Defense Technology.

[53] Xiao Tianliang [肖天亮], ed., *The Science of Military Strategy* [战略学] (Beijing: National Defense University Press [国防大学出版社], 2017). The PLA initially concentrated on space and cyberspace as new strategic frontiers of military power. Increasingly, biology and intelligent confrontation have been recognized as new domains of military struggle in which the Chinese military, as a latecomer is seeking to catch up with a powerful adversary.

[54] LI Bicheng [李弼程], HU Huaping; [胡华平], and XIONG Yao [熊尧], “Intelligent agent model for network public opinion guidance” [网络舆情引导智能代理模型], National Defense Technology [国防科技], no. 3, (2019).

[55] Lan Zhouda [兰舟达] and Ma Jianguang [马建光], “A New Type of Cyber Warfare from the Perspective of Mental Dominance—Taking the Color Revolution as an Example” [制脑权视野下的新型网络战—以颜色革命为例], *National Defense Science and Technology* [国防科技] 36, no. 2 (2015): 57–62, available at <http://gfkjjournal.nudt.edu.cn/ch/reader/view_abstract.aspx?file_no=20150212&flag=1>.

[56] Luo Xu [罗旭], Wu Hao [吴昊], and Guo Ji-wei [郭继卫], “Research on a Systematic Framework for Brain Science Military Applications for New-Type Combat Forces Construction Strategy” [论新型作战力量战略下的脑科学军事应用体系构成研究], *Military Medicine* [军事医学] 11 (2015): 863–867.

[57] “‘Brain Plan’ Opens ‘Mental Dominance’ into a New Highland for Future Military Contests” [“脑计划”开启 “制脑权”成未来军事较量新的高地], *PLA Daily*, October 20, 2016, available at <http://military.people.com.cn/n1/2016/1020/c1011-28793350.html>.

[58] See, for instance Shen and Zhang, “Understanding Intelligentized Operations.”

[59] Ibid.

[60] Ibid.

[61] See “Brain Science Sociology and Brain-Computer Interface Technology Series Academic Report” [“脑科学与脑机接口技术”系列学术报告], May 15, 2019.

[62] Since the PLA reforms, this team is now included

under NUDT's Institute for Intelligent Science and Technology; "'Brain-Machine Interface' Technology: Making 'Brain Control' a Reality" ["脑机接口" 技术：让 "脑控" 成为现实], China Military Online, May 21, 2015, available at <http://www.mod.gov.cn/wqzb/2015-05/21/content_4586049_2.htm>.

[63] His research on the theme of "brain networking and brain-computer interaction" has been awarded, and his influence appears to have deeply shaped the field: see "Military School Scratches 'Cool Smart Wind.'"

[64] "'Brain Plan' Opens 'Mental Dominance' into a New Highland for Future Military Contests."

[65] "'Brain-Machine Interface' Technology Coming from the Laboratory into Real Life" ["脑机接口" 技术正从实验室走进现实生活], available at <http://www.stdaily.com/cxzg80/guonei/2017-12/28/content_614787.shtml>. See also:http://www2.scut.edu.cn/bci/2018/0910/c18577a284388/page.htm>.

[66] "Human-Machine Cooperation Entering Actual Combat Intelligentization or Starting from the Laboratory" [人机协同投入实战 智能化战争或从实验室打响], *S&T Daily*, June 26, 2019.

[67] "The Ministry of Education Convened a Press Conference to Interpret the Artificial Intelligence Innovation Action Plan for Colleges and Universities, etc." [教育部举行新闻发布会解读《高等学校人工智能创新行动计划》等], Ministry of Education website, June 8, 2018, available at <http://www.gov.cn/xinwen/2018-06/08/content_5297021.htm#2>.

[68] "Special Action Plan for Military-Civil Fusion in the Domain of Intelligent Science and Technology in Tianjin" [天津市智能科技领域军民融合专项行动计划], August 9, 2018, available at <https://web.archive.org/web/20190918010942/http://gyxxh.tj.gov.cn/zhencwj/65062.htm>.

[69] China Aerospace Science and Technology Corporation (CASC),"Tianjin University 'Intelligence' Helps China Aerospace" [天大 "智" 造助力中国航天], March 23, 2018, available at <http://news.tju.edu.cn/info/1003/22110.htm>.

[70] "State Key Laboratory of Cognitive Neuroscience and Learning Held the 2018 Academic Committee Meeting" [认知神经科学与学习国家重点实验室召开2018年学术委员会会议], January 16, 2019, available at <http://brain.bnu.edu.cn/cn/tza/2019/0116/1424.html>.

[71] 2019 World Robotics Conference BCI Brain-Control Robotics Competition and Third China Brain-Machine Interface Competition [2019世界机器人大赛—BCI脑控机器人大赛暨第三届中国脑机接口大赛], World Robotics Conference, available at <https://web.archive.org/web/20191011041722/http://2018.worldrobotconference.com/uploads/file/20181224/15456436152616.pdf>.

[72] See, for instance, comments from Cogrowth founder and CEO Hua Zhongling, available at <http://www.naokexue.com.cn/news/gs/187.html>.

[73] "China Unveils Brain-Computer Interface Chip," *Xinhua*, May 18, 2019, available at <http://www.xinhuanet.com/english/2019-05/18/c_138069590.htm>.

[74] "Brain-Computer Interface and Intelligent Control and First Brain Science Seminar Held" [脑机接口与智能控制暨首届脑科学研讨会举行], *Economics Daily* [经济日报], December 25, 2017, available at <http://www.ce.cn/cysc/yy/hydt/201712/25/t20171225_27421101.shtml>.

[75] Ibid. According to its designer, "Brain-Computer Interfaces hold a promising future. The Brain Talker chip advances BCI technology allowing it to become more portable, wearable, and accessible to the general public."

[76] Ibid.

[77] "Shape the 'Combat Brain' for the Future—How Far Is 'Brain Networking' from Us?" [为未来塑造 "作战大脑" "脑联网" 离我们有多远?], *PLA Daily* [解放军报], December 22, 2017, available at <https://www.chinanews.com/cj/2017/12-22/8406674.shtml>.

[78] "Academy of Military Medical Sciences Researcher Wu Haitao Explains to You 'What Will Brain Science Bring from the Military'" [军事科学院军事医学研究院研究员吴海涛为您讲述——脑科学 "从军" 会带来什么?], available at <http://www.81.cn/jfjbmap/content/2019-04/26/content_232600.htm>.

[79] Yipeng Yu et al., "Intelligence-Augmented Rat Cyborgs in Maze Solving," *PloS One* 11, no. 2 (2016): e0147754.

[80] The Chinese government's decision to prioritize brain science can be traced back to the National Medium- and Long-Term Plan for Science and Technology Development (2006–2020), which had emphasized the importance of strengthening the study of the relationships among brain development, plasticity, and human intelligence. At the time, this initiative constituted one of the "Major Science and Technology Projects Concerning China's Future Development" (事关我国未来发展的重大科技项目). Through the 13th Five-Year Science and Innovation Plan, there were megaprojects launched in brain science and brain-inspired intelligence, as well as artificial intelligence for the 2016–2030 timeframe. See "National Medium and Long Term Science and Technology Development Plan Outline" (2006–2020) [国家中长期科学和技术发展规划纲要], Ministry of Science and Technology, February 9, 2006, available at <http://www.most.gov.cn/mostinfo/xinxifenlei/gjkjgh/200811/t20081129_65774_9. Htm>. See also "Our Nation Launched Four Major Science Research Programs" [我国启动四项重大科学研究计划], *Science and Technology Daily*, November 16, 2006.

[81] "Notice of the State Council on the Printing and Distribution of the Thirteenth Five-Year National Science and Technology Innovation Plan" [国务院关于印发"十三五"国家科技创新规划的通知], State Council, August 8, 2016, available at <http://www.gov.cn/zhengce/content/2016-08/08/ content_5098072.htm>.

[82] Starting in 2013, the Chinese government had decided to launch the "China Brain Project" (中国脑计划), but its actual launch was not formalized until 2016, and the development of a plan for its implementation seems to have been further delayed. However, there have been initial research programs and laboratories launched in Beijing and Shanghai that are intended to advance this agenda.

[83] "Neurobiologist Pu Muming: How Brain Science Helps AI Technology Research" [神经生物学家蒲慕明：脑科学如何助力AI技术研究], Netease Intelligence [网易智能], April 27, 2018, available at <http://tech.163.com/18/0427/12/DGD9O89000098IEO.html>.

[84] The emphasis on hybrid intelligence is not merely a concept but also a priority in the New Generation Artificial Intelligence Development Plan, released in July 2017, which emphasized China's intention to pursue significant breakthroughs in hybrid enhanced intelligence and human-machine interaction: "Research hybridization and convergence where "the human is in the loop," behavioral strengthening through human-machine intelligent symbiosis and brain-machine coordination, intuitive machine reasoning and causal models, associative recall models and knowledge evolution methods, complex data and task blended and enhanced intelligence learning methods, cloud robotics coordination computing methods, and situational comprehension and human-machine group coordination in real-world environments."

[85] See "Beijing Brain Science Research Is Constantly Turning Research Results into Reality" [北京脑科学研究正不断将研究成果转化成现实], January 12, 2016, available at <http://news.sciencenet.cn/htmlnews/2016/1/335972.shtm>. This initiative involves units that include the Chinese Academy of Sciences Institute of Automation and the Academy of Military Medical Sciences, as well as Peking University and Tsinghua University. For further information, see "Beijing Brain Science and Brain-like Research Center Postdoctoral Science and Research Work Station 2019 Application Announcement [北京脑科学与类脑研究中心博士后科研工作站2019年招聘启事], available at <http://www.chinapostdoctor.org.cn/content/details20_690.html>; "Beijing Launches Pioneering Brain Science Center," Scientific American, 2016, available at <https://www.scientificamerican.com/article/beijing-launches-pioneering-brain-science-center/>.

[86] "Thirteenth Five-Year Science and Technology Military-Civil Fusion Development Special Plan" (Full Text) ["十三五"科技军民融合发展专项规划》全文], available at <http://www.aisixiang.com/data/106161.html>.

[87] Jing Pei et al., "Towards Artificial General Intelligence with Hybrid Tianjic Chip Architecture," *Nature* 572, no. 7767 (2019): 106. Of course, it remains to be seen whether these brain-inspired approaches to artificial intelligence prove to be a promising architecture. According to the researchers, "The brain-like intelligence inspired by the operating mechanism and cognitive behavior can make up for the limitations and shortcomings of current data intelligence. More critically, brain-like intelligence will subvert the traditional computer operating architecture, achieve a new computing and storage integration model, and is expected to achieve ultra-low power consumption."

[88] "Xiangshan Science Conference on 'Non-human Primate Brains and Cognition' Held" [香山科学会议"非人灵长类脑与认知"召开].

[89] See, for instance, "Where Is the Winning Mechanism of Intelligent Warfare?" [智能化战争的制胜机理变在哪里], *PLA Daily*, January 15, 2019, available at <http://www.xinhuanet.com/mil/2019-01/15/c_1210038327.htm>.

[90] Although this program has not been officially disclosed or announced, available references to it provide robust indications that this project is underway.

[91] Ibid.

[92] "Brain Region Linked to Altered Social Interactions in Autism Model," McGovern Institute for Brain Research, July 29, 2019, available at <https://www.sciencedaily.com/releases/2019/07/190729094551.htm>.

[93] Ibid.

[94] Feng Zhengzhi [冯正直] and Zhang Rui [张 睿], "Progress in Military Cognitive Neuroscience" [军事认知神经科学研究进展], PhD diss., 2013. The authors are affiliated with the Department of Behavioral Medicine, College of Psychology, Third Military Medical University.

[95] The original article is no longer readily available, but see a reference to the <https://webcache.googleusercontent.com/search?q=cache:-Ih4uFfS-RXwJ:https://www.shobserver.com/wx/detail.do%3Fid%3D86079+&cd=3&hl=en&ct=clnk&gl=us>.

[96] Mu-ming Poo et al., "China Brain Project."

[97] Ibid. This massive scaling up of capacity for primate research nationwide with robust state support could provide a potential advantage relative to the United States and Europe. In China, researchers can benefit from the ease, low cost, and speed of research without attendant controversies.

[98] "Xiangshan Science Conference on 'Non-human

Primate Brains and Cognition' Held."

[99] For instance, researchers at the Academy of Military Medical Sciences are using macaques to examine techniques for brain-machine interfaces that involve the implantation of electrodes in the brain.

[100] Antonio Regalado, "Chinese Scientists Have Put Human Brain Genes in Monkeys—And Yes, They May Be Smarter," *MIT Technology Review*, April 10, 2019, available at <https://www.technologyreview.com/s/613277/chinese-scientists-have-put-human-brain-genes-in-monkeysand-yes-they-may-be-smarter/>; Sigal Samuel, "Scientists Added Human Brain Genes to Monkeys. Yes, It's as Scary as it sounds," *Vox*, April 12, 2019, available at <https://www.vox.com/future-perfect/2019/4/12/18306867/china-genetics-monkey-brain-intelligence>.

[101] Lei Shi et al., "Transgenic rhesus Monkeys Carrying the Human MCPH1 Gene Copies Show Human-like Neoteny of Brain Development," *National Science Review* 6, no. 3 (2019): 480–493.

[102] "Scientists Are Making Human-Monkey Hybrids in China," *MIT Technology Review*, August 1, 2019, available at <https://www.technologyreview.com/s/614052/scientists-are-making-human-monkey-hybrids-in-china/>.

[103] See Manuel Ansede, "Científicos españoles crean quimeras de humano y mono en China," July 30, 2019, available at <https://elpais.com/elpais/2019/07/30/ciencia/1564512111_936966.html>.

[104] Hao Wang et al., "CRISPR/Cas9 System: An Important Tool for Brain and Cognitive Science," *Progress in Biochemistry and Biophysics* 44, no. 9 (2017): 799–805, available at <http://www.pibb.ac.cn/pibbcn/ch/reader/create_pdf.aspx?file_no=20170237>.

[105] For an earlier collaborative analysis on the topic, see Elsa Kania and Wilson VornDick, "China's Military Biotech Frontier: CRISPR, Military-Civil Fusion, and the New Revolution in Military Affairs," *China Brief* 19, no. 18, available at <https://jamestown.org/program/chinas-military-biotech-frontier-crispr-military-civil-fusion-and-the-new-revolution-in-military-affairs/>.

[106] See Guo Jiwei (郭继卫), *War for Biological Dominance* (制生权战争) (Beijing: Xinhua Press, 2010).

[107] Li Hong-jun and Guo Ji-wei, "Evolution of Forms of Warfare Promoted by Modern Biotechnology" [现代生物科技推动战争形态演变的思考]. The authors are affiliated with the Southwest Hospital of the Third Military Medical University.

[108] Lou Tie-zhu [楼铁柱], "Review and the Outlook for Military Applications of Synthetic Biology" [合成生物学发展回顾与军事应用前景展望], Institute of Health Service and Medical Information, Academy of Military Medical Sciences.

[109] Beyond outright military research, there is an emerging ecosystem of academic and commercial enterprises that are or could become involved in supporting military research. See "Thirteenth Five-Year Science and Technology Military-Civil Fusion Development Special Plan."

[110] Yi Biyi [易比一] et al., "Concept Research of Zhishengquan" [制生权概念研究], Military Medical Science [军事医学] 42, no. 1 (January 2018).

[111] See Lu Peipei [陆倍倍] and He Fuchu [贺福初], "Biological Science and Technology Will Become the Strategic Commanding Heights of the Future Revolution in Military Affairs" [生物科技将成为未来军事革命新的战略制高点], *PLA Daily*, October 6, 2015, available at <https://web.archive.org/web/20190813042422/http://www.81.cn/jwgz/2015-10/06/content_6709533.htm>.

[112] Ibid.

[113] Ibid.

[114] He Fuchu, "The Future Direction of the New Global Revolution in Military Affairs."

[115] Indeed, the phrasing is repeated more or less verbatim in this book by General (Ret.) Zhang Shibo (张仕波), former commandant of the PLA's National Defense University Zhang Shibo [张仕波], *The New High Ground* [新高地] (Beijing: National Defense University Press, 2017). I am indebted to Wilson VornDick for drawing this book to my attention.

[116] See, for instance: Zeng Huafeng [曾华锋] and Shi Haiming [石海明], "Scientific and Technological Deterrence: A New Trend in the Use of Military Power" [科技威慑：军事力量运用的新趋势], February 17, 2019, available at <http://www.sohu.com/a/295253193_358040, http://opinion.people.com.cn/n1/2018/0204/c1003-29804335.html>.

[117] Fang [李芳] and Shi Haiming [石海明], "Biology and Interdisciplinary Technologies" [生物交叉技术：撬动生理信息战的前沿科技], *Guangming Network, Military Technology Frontier* [军事科技前沿], October 19, 2016, available at <http://junshi.gmw.cn/2016-10/19/content_23026987.htm>.

[118] Ibid.

[119] That is, certain of these writings are vague, likely deliberately, about whether their purpose is to raise concerns that China could be subject to these kinds of attacks or to highlight their offensive potential as a direction of development that China should pursue going forward.

[120] David Cyranoski, "Chinese Scientists to Pioneer First Human CRISPR Trial," *Nature News* 535, no. 7613 (2016): 476, available at <https://www.nature.com/articles/nature.2016.20302>; Jon Cohen, "The CRISPR Animal Kingdom," *Science*, August 2, 2019, 426–429, available at

<https://science.sciencemag.org/content/365/6452/426.summary>.

[121] Caixia Gao, "The Future of CRISPR Technologies in Agriculture," *National Review of Molecular Cell Biology* 19, no. 5 (2018): 275–276.

[122] See, for instance, "Safety of Transplantation of CRISPR CCR5 Modified CD34+ Cells in HIV-infected Subjects with Hematological Malignances (NCT03164135)," sponsored by Affiliated Hospital to Academy of Military Medical Sciences, Study Evaluating UCART019 in Patients with Relapsed or Refractory CD19+ Leukemia and Lymphoma (NCT03166878), Chinese PLA General Hospital.

[123] Further details are available upon request.

[124] Ibid. Further details are available upon request.

[125] Michael Specter, "The Gene Factory," *The New Yorker*, December 29, 2013, available at <https://www.newyorker.com/magazine/2014/01/06/the-gene-factory>.

[126] For context, see John Bohannnon, "Why Are Some People So Smart? The Answer Could Spawn a Generation of Superbabies," *Wired*, July 2013, available at <https://www.wired.com/2013/07/genetics-of-iq/>. Similarly, another company, Beijing Xinuo Valley Biotechnology Co. Ltd., has cloned a number of dogs as pets and for policing. "This Cloned Dog Is Too Superior" [这只被克隆狗太优秀], *Netease S&T*, August 22, 2019, available at <https://web.archive.org/web/20190914070025/https://www.cnbeta.com/articles/tech/881183.htm>.

[127] Shen Bin et al., "Efficient Genome Modification by CRISPR-Cas9 Nickase with Minimal Off-target Effects," *Nature Methods* 11, no. 4 (2014): 399.

[128] For context, see BGI's website and promotional materials, available at <https://www.bgi.com/global/>.

[129] See this great project from the Australian Strategic Policy Institute: "China's Tech Expansion," available at <https://chinatechmap.aspi.org.au/#/company/bgi>.

[130] This claim was included in a news article that is not entirely authoritative, but constitutes an interesting characterization of that decision.

[131] Emma Yasinki, "China Clamps Down on Foreign Use of Chinese Genetic Material and Data," *The Scientist*, June 17, 2019, available at <https://www.the-scientist.com/news-opinion/china-clamps-down-on-foreign-use-of-chinese-genetic-material-and-data-66016>.

[132] Cui Yingbo et al., "Review of CRISPR/Cas9 sgRNA Design Tools," *Interdisciplinary Sciences: Computational Life Sciences* 10, no. 2 (2018): 455–465.

[133] Further details are available upon request.

[134] Yang Xi et al., "An Interface for Biomedical Big Data Processing on the Tianhe-2 Supercomputer," *Molecules* 22, no. 12 (2017): 2116.

[135] Cui et al., "Review of CRISPR/Cas9 sgRNA Design Tools."

[136] Mason Marks and Tiffany Li, "DNA Donors Must Demand Stronger Protection for Genetic Privacy," *StatNews*, May 30, 2018, available at <https://www.statnews.com/2018/05/30/dna-donors-genetic-privacy-nih/>.

[137] James M. Sikela, "The Jewels of our Genome: The Search for the Genomic Changes Underlying the Evolutionarily Unique Capacities of the Human Brain," *PLoS Genetics* 2, no. 5 (2006): e80, available at <https://doi.org/10.1371/journal.pgen.0020080>.

A U.S. Air Force MQ-9 Reaper remotely piloted aircraft equipped with external fuel tanks and armed with munitions sits in a hanger prior to Intelligence, Surveillance, and Reconnaissance operations at Ali Al Salem Air Base, Kuwait, July 23, 2019. (Tech. Sgt. Michael Mason))

Killing Me Softly
Competition in Artificial Intelligence and Unmanned Aerial Vehicles

By Norine MacDonald and George Howell

The conduct of war is being fundamentally altered by the revolutionary impact of artificial intelligence (AI). The competition in AI and unmanned aerial vehicles (UAVs) marks the onset of the "7th Military Revolution" and the states that integrate these advances first will have a prodigious military advantage."[1] China has seized this moment, increasingly posing a risk to the historical technological advantage of the United States and destabilizing the foundations of modern warfare.

China has invested extensively in artificial intelligence and used significant aggressive covert and overt technological appropriation to rapidly revolutionize its military capabilities. China's innovation on the military front is mirrored by its national commitment to achieving superiority in the civilian and commercial applications of AI systems. The United States not only risks falling behind in the AI arms race but also is in danger of losing its commanding edge in commercial AI, where the Chinese government has committed vast amounts of capital to achieving dominance in AI applications across the economy. For example, China was the source of most cited high-impact research papers on AI in 2018 and has demonstrated an efficient strategy of technological capacity appropriation and civil-military fusion to build advanced defense capabilities.[2]

This is augmented by not only a specific alignment with Russia, but also a deepening of infrastructural and financial ties with Pakistan (the world's specialist in mini-nuclear weapons).[3] A consolidation of influence through infrastructural development in Central Asia and Africa, through the Belt and Road Initiative, as well as growing defense relationships in the Gulf region, with deepening ties with the United Arab Emirates and Saudi Arabia, are cases in point. Through such global efforts China is establishing strategic alliances together with a global technology infrastructure of satellites, undersea cables, and wireless networks that will support the capacity of its unmanned artificial intelligence–empowered system.[4]

The emergent battlefield will be a contested electromagnetic environment requiring adaptability across the battle network and intensive integration in order to exploit weaknesses in enemy networks and penetration points while protecting one's own. Systems designed for the historical asymmetric context will no longer be suitable and will have to be repurposed. There must be both multi-domain situational awareness and the ability to rapidly follow up with strike, swarming, and anti-swarming capabilities.

Norine MacDonald Q.C. is a Visiting Distinguished Research Fellow, INSS, National Defense University and founder of RAIN Research. George Howell is a policy analyst and co-founder of RAIN Research, focusing on the nexus between artificial intelligence and strategic defense issues.

This study of the current range of UAVs, and the ways in which AI can enhance them, offers a specific consideration of the metamorphosis of the battlespace—what one can expect competitors to field, and what sort of response will be required. We do not reference the creation of a general AI but the extensive, consolidated use of narrow AI to integrate, process, and sort the vast amounts of accumulated and incoming data at all levels of the military enterprise.[5] Unmanned systems must be empowered with AI capability to enable swarming, teaming, and sensor interpretation.

There must be both reimagining of the conduct of warfare and adding new methodologies for managing and developing these breakthroughs. Both an AI core and AI "nervous system" are needed, with an accompanying integration of systems and networking capacity. As former Commander, U.S. Special Operations Command General Raymond Thomas has noted,

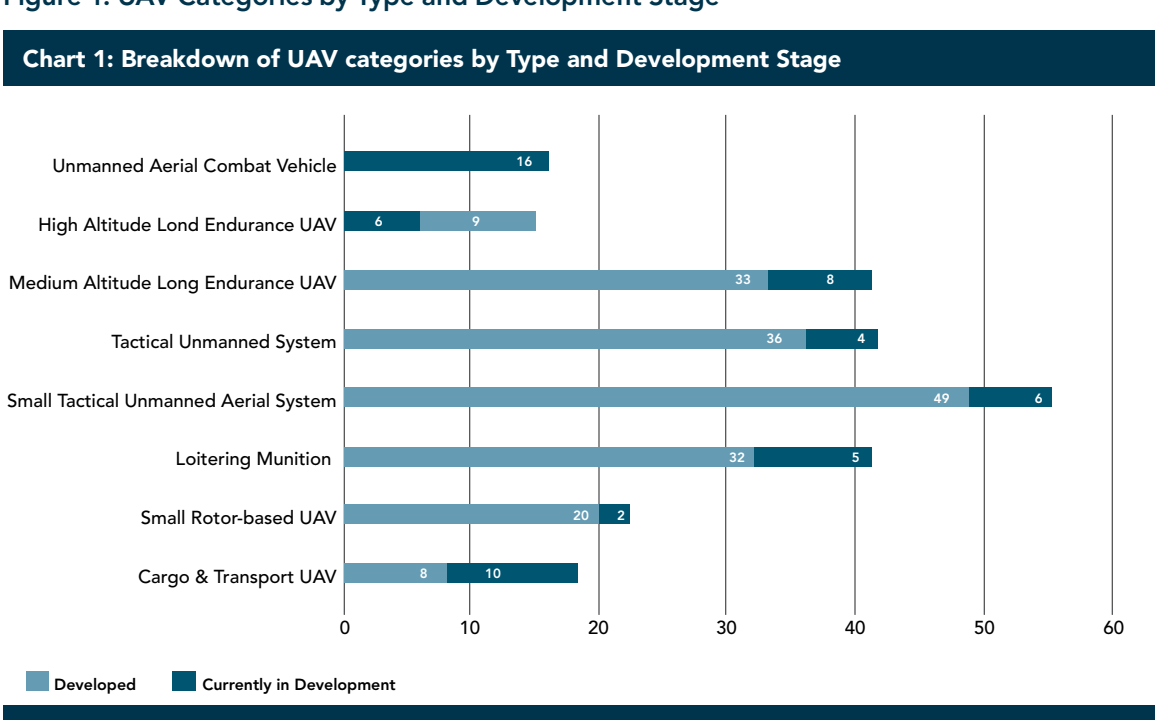
> *We have a conflation of opportunities in terms of unmanned that is extraordinary. Unmanned everything, ships, ground mobility vehicles, aircraft it's almost limitless. I visualize you can do almost all of that unmanned in the near future.*[6]

This UAV research serves as another alert call to the danger of becoming a technological laggard in the new battlespace in the face of an industrious, focused, innovative challenger.

UAV Classification System

This article is informed by open source research on prevalent unmanned systems available globally, conducted between February and August 2019, in

Figure 1. UAV Categories by Type and Development Stage



Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

an original taxonomy of more than 250 platforms, focusing on the integration of AI with such systems.[7] We offer a presentation of the characteristics of the different platforms of UAVs and an analysis of the pivotal impact of AI in such systems. The breakdown differs from the Department of Defense classification by weight, altitude, and speed in order to bring a more detailed description to the smaller platforms.[8]

The breakdown of UAV systems available is shown in Table 1. Small tactical systems are the most common, followed by rotor-based larger tactical systems and loitering munitions. Many medium-altitude long endurance (MALE) UAVs are available. There are currently very few high-altitude long endurance (HALE) UAVs, but more are on the way. All unmanned combat aerial vehicle (UCAV) projects are still in development. A brief description of each of the categories follows.

UCAVs in Development

The UCAV segment will be the largest of all military UAV segments in the 2018 to 2028 period, estimated at $57 billion and accounting for 39 percent of the $153 billion cumulative global market.[9] This demonstrates the strategic importance of the UCAV that is related to the potential ease that such platforms could be combined with nuclear payloads. The research dataset shows a total of 16 projects being developed around the world, with the United States having 37 percent of the global total and China following closely with 31 percent. India, Russia, the United Kingdom, and a European consortium have one project each.

Most UCAVs are Flying Wing stealth designed and generally look very similar to the RQ-170 Sentinel surveillance HALE-class UAV that landed in Iran in 2011.[10] The result was a technology leap by Iran and others. UCAVs aim to penetrate denied area spaces, which is indicative of the global push toward fielding

Table 1. Unmanned Combat Aerial Vehicles

Purpose
Intelligence, Surveillance, Reconnaissance (ISR): 7%
Weapons Systems: 75%
(Guided Missiles, Precision Bombs, potential nuclear payloads and small UAV swarms)

	Total (273)	Weaponized	Unarmed	ISR	ISTAR	EW	Relevant AI	Sector Specific Factors	Top Companies	Producer Countries (share of global total)	Operator
UCAV	16	12 (Bombers)	4	3	6	3	Auto-mission: 16 (100%) MUM-T: 8 (50%) ATOL AI Combat algorithms	Stealth: 11 (62%) Attainable: 2 (16%) Hypersonic: 2 (16%) Refueling: 1	Boeing, Lockheed Martin Northrop Grumman, BAE, AVIC, CASC, CASIC	USA (37%) China (31%)	Air Force Navy
In Dev	0	75%	25%	18%	6	18%					
	EW is Electronic Warfare, MUM-T is Manned/Unmanned Teaming, ATOL is Automatic Take-off and Landing AVIC is Aviation Company of China, CASC is China Aerospace Science and Technology Corporations, CASIC is China Aerospace Science and Industry Corporation, BAE is British Aerospace Engineering Total UAVs is dataset: 273/Total UCAVs: 16										

Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

UAVs for use in near-peer competition. The missions of such aircraft are predominantly strategic bombing and covert intelligence, surveillance, and reconnaissance (ISR) missions.

Three different talents define the UCAV segment: stealth (to gain access to enemy territory undetected), hypersonic speed and agility, and serving as an "attritable aerial asset," meaning a disposable apparatus that can be locally controlled by aircraft pilots. In this review, we found that 11 of 16 are designed for the stealth approach, only China and the United States are currently involved in hypersonic projects, and three attritable aerial assets are being developed—two in the United States and one in Australia.

HALE UAVs

HALE systems are characterized by satellite control links and a high operational ceiling, operating for long periods of time and having the capability of surveying very large areas. A well-known specimen is the Northrop Grumman Triton, which can scan 100,000 square meters a day and stay airborne for more than 30 hours at a time.[11] Such systems conduct long-range ISR and intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) missions, as well as being used for battle network communication and increasingly for electronic warfare. This provides persistent near-real-time coverage using imagery intelligence, signals intelligence, and moving target indicator sensors.

In their current form, HALE systems deployed by the United States are suited for asymmetric warfare environments and global scanning rather than conflicts involving anti-access/area denial (A2/AD) capabilities. The Global Hawk has suffered in contested environments, as the downing of the vehicle in June 2019 by an Iranian surface-to-air

Table 2. High-Altitude Long Endurance UAVs

Purpose
Intelligence, Surveillance, Reconnaissance (ISR): 33%
Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR): 66%
Weapons Systems: 50% (Surface to Ground Missiles)

	Total (273)	Weaponized	Unarmed	ISR	ISTAR	EW	Relevant AI	Sector Specific Factors	Top Companies	Producer Countries (share of global total)	Operator
HALE Developed	6	3	3	2	4	2	Autonomous Flight Mode: (RQ170)	Stealth: 1 Hybrid VTOL: 1	Northrop Grumman Lockheed Martin General Atomics	USA 4 China 2	Air Force Navy
HALE In Dev	9	3	4	7	0	0		Solar: 3 (27%) Hydrogen Powered: 1	AVIC Boeing Lockheed Martin Northrop Grumman	USA: 5 (63%) China: 3 (45%)	Air Force Navy
	EW is Electronic Warfare AVIC is Aviation Company of China Total UAVs is dataset: 273/Total UCAVs: 16										

Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

missile demonstrated.[12] Following that incident, India backtracked on a deal to purchase the platform because of perceived ineffectiveness in a potential conflict with A2/AD-enabled Pakistan.[13] Northrop Grumman is adapting the Global Hawk with longer range sensors to allow it to operate in contested environments. However, the issue with the platform is that it was not designed for near-peer competition, illustrating an opening for a next stage product.[14]

China's Aviation Industry Corporation (AVIC) recently introduced two sensor laden HALEs with the capability of airborne warning and control systems (AWACS), specifically the detection of stealth aircraft. The Soar Dragon and Divine Eagle are also equipped with anti-ship missiles.[15] Chinese AWACS technology is advanced, and the possibility of detection by such aircraft undermines the viability of the F-35 as a radar-evading platform.[16] A Soar Dragon was used to track the movements of a U.S. cruiser in the Taiwan Strait in June 2019.[17]

MALE UAVs

The MALE segment of UAVs is the most well-known strike-capable UAV, made famous by the General Atomics Predator platform. Sixty percent of MALE platforms found had weapons capabilities, and 96 percent of those include precision and anti-armor strikes. Ninety-six percent of platforms had the purpose of situational awareness through ISR or ISTAR missions. Such systems include sensor equipment such as synthetic aperture radar, thermal and infrared sensors, and live video feed transmission capabilities.

China has a high number of MALE platforms that are actively marketed for export, such as the AVIC Wing Loong platform and the China Aerospace

Table 3. Medium-Altitude Long Endurance UAVs

Purpose
Intelligence, Surveillance, Reconnaissance (ISR): 33%
Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR): 63%
Weapons Systems: 60% (Precision Bombs, Air to Surface Missiles)

	Total (273)	Weaponized	Unarmed	ISR	ISTAR	EW	Relevant AI	Sector Specific Factors	Top Companies	Producer Countries (share of global total)	Operator
MALE Developed	33	20 60%	13 40%	11 33%	21 63%	3 25%	ATOL: 2 (6%) No pilot-ing skills required: 1 Autonomous Flight: 2	Denied Area Access: 1 Can launch loitering munition: 1 (Belarus) Hybrid VTOL: 1	AVIC CASC General Atomics IAI	China: 12 (26%) Israel: 7 (21%) USA: 5 (15%)	Air Force Navy Army
MALE In Dev	8	6 75%	2 25%	1 12.5%	6 75%	2 25%	ATOL: 1 (Russia/ Orion) (12.5%)			Turkey: 2 (25%) USA: 1 China: 1	Air Force Navy Army Divisions
	EW is Electronic Warfare, ATOL is Automatic Take-off and Landing AVIC is Aviation Company of China, CASC is China Aerospace Science and Technology Corporation, IAI is Israel Aerospace Industries Total UAVs is dataset: 273/Total MALE UAVs: 41										

Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

Science and Technology Corporation (CASC) CH-4. CASC has established factories for the CH-4 platform in Pakistan, Myanmar, and Saudi Arabia.[18] In addition, China is developing a MALE UAV for early warning, a stealthy AWACS-empowered MALE platform, and the JY-300 Tian Shao.[19] This allows for greater situational awareness and battlefield intelligence on an inexpensive and agile platform.

It is noteworthy that China significantly leads the MALE export field (225), according to the Stockholm International Peace Research Institute arms transfer database for exports between 2012 and 2018, followed by Israel (137) and the United States (51).[20]

Tactical Unmanned Aircraft Systems

Tactical unmanned aerial systems function as air support for ground forces, providing situational awareness to the warfighter. Agility is a key factor of such systems, and a hybrid fixed-wing and vertical take-off (VTOL) capability is the growing trend. The advantage of fixed-wing over rotor-based systems is aerodynamic efficiency, because such systems can stay in the air longer and can scan a wider area. However, they have more difficulty hovering in one place. The hybrid-VTOL models that combine rotors with a fixed-wing design offer dual loitering and wide area scanning capabilities. Only 16 percent of

Table 4. Tactical Unmanned Aerial Systems

Purpose
Intelligence, Surveillance, Reconnaissance (ISR): 66%
Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR): 22.2%
Weapons Systems: 16% (Light Missiles)

	Total (273)	Weaponized	Unarmed	ISR	ISTAR	EW	Relevant AI	Sector Specific Factors	Top Companies	Producer Countries (share of global total)	Operator
TUAS Developed	36	6 16%	30 84%	24 66%	8 22.2%	1 2.7%	ATOL: 5 (13.8%) Autoflight: 3 Pattern of life recognition: 1 MUM-T: 1	Fixed Wing: 29 (80%) Hybrid VTOL: 7 (19.4%) Denied Area Access: 1 Perimeter Defense: 1 IED Detection: 1 Cargo drops: 1	Insitu (Boeing) L-3 Harris Latitude Textron IAI	USA: 12 (33%) China: 3 (8.3%) Israel: 3 (8.3%)	Navy Army Brigades
TUAS In Dev	4	2 50%	2 50%		2 50%	1 25%		Hybrid VTOL: 3 (75%) Fixed Wing: 1	Textron Luch Design Bureau Pterodynamics	USA: 2 (50%) Russia: 1 (25%) Latvia: 1 (25%)	Navy Army Brigades
	EW is Electronic Warfare, ATOL is Automatic Take-off and Landing, MUM-T is Manned/Unmanned Teaming Total UAVs is dataset: 273/Total TUAS: 40										

Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

platforms currently available are weaponized. The number increases to 50 percent when reviewing platforms in development.

Small Tactical Unmanned Aircraft Systems

Small tactical unmanned aircraft systems can be linked with unmanned ground sensors and automatically take off and fly to the sensor location, as seen with South Korea's Vivace system, or can locate and intercept cell-phone signals, as in the case of Israel's Aeronautics Orbiter 4 system.[21] The MBDA Spectre currently in development offers a small weaponized system suitable for contested environments.[22]

Table 5. Small Tactical UAS Systems

Purpose
Intelligence, Surveillance, Reconnaissance (ISR): 25%
Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR): 51%
Weapons Systems: 49% (Small Missiles in development)

	Total (273)	Weaponized	Unarmed	ISR	ISTAR	EW	Relevant AI	Sector Specific Factors	Top Companies	Producer Countries (share of global total)	Operator
STUAS Developed	49	0	49 100%	25 51%	24 49%	2 4%	ATOL: 4 (8%) Auto-mission: 1 MUM-T: 1 Object Recognition: 1 Sensor-link auto launch: 1 Interface simplification: 1 Machine vision: 1 (Vidar)	Catapult Launch: 23 (65%) Hand Launched: 18 (36%) Hybrid VTOL: 6 (12%) Cellular interception: 1 Denied Area Access: 4 Perimeter Defense: 2 Solar: 2 Cargo drops: 2	AeroVironment: 4 CASC: 4 Aeronautics: 3	USA: 17 (34%) Israel: 9 (18%) China: 5 (10%)	Navy Marines Army Battalions
STUAS In Dev	6	2 33%	4 66%	3 50%	2 33%	2 33%	Auto flight: 1 (16.6%) Swarming: 1 (16.6%) MUM-T: 1 (16.6%)	Hybrid VTOL: 4 Disguised: 1	MBDA Textron	USA Europe Russia	Navy Marines Army Battalions
	EW is Electronic Warfare, ATOL is Automatic Take-off and Landing, MUM-T is Manned/Unmanned Teaming CASC is China Aerospace Science and Technology Corporation, Total UAVs is dataset: 273/Total STUAS: 55										

Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

Loitering Munitions

Loitering munitions are a diverse segment of UAVs that can be piloted or pre-programmed to strike specific targets. The larger versions can loiter for longer, while smaller versions are mostly pneumatically tube-launched and have an air-time capacity of approximately 20 minutes. Such systems can weigh as little as 3 kilograms and can be piloted on a cell phone device. In addition, small multi-rotor variations are available. Many offer precise strikes with around a 1-meter radius, and others have anti-tank warhead capabilities.

Table 6. Loitering Munitions

Purpose
Weaponized: 100%

	Total (273)	Weaponized	Unarmed	ISR	ISTAR	EW	Relevant AI	Sector Specific Factors	Top Companies	Producer Countries (share of global total)	Operator
Loitering Munition Developed	32 Large: 8 Small: 24	32 100%	0			4 12.5%	Autonomous strike capability: 9 (28%) Semi-automatic flight: 9 (28%) AI enabled tracking: 4 (12.5%) Object identification: 3 (9.3%) Swarming: 4 (12.5%)	Pneumatic Tube launched: 16 (50%) Armor Piercing: 4 (12.5%) Vehicle launched: 5 (15%) Air Launched: 4 Small Rotor based: 3 Grenade design: 1 Mini helicopter: 1	IAI: 5 Uvision: 5	Israel: 13 (40%) USA: 4 (12.5%) China 4 (12.5%)	Air Force Navy Army Large-sized Battalions Small-sized Squads
Loitering Munition In Dev	5 Large: 2 Small: 3	5 100%	0				Swarming: 1 (20%) Autonomous Strike capability: 1 (20%)	Air launched: 2 Armor Piercing: 1 Pneumatic Tube Launched: 3		South Korea Turkey India	Air Force Navy Army Large-sized Battalions Small-sized Squads
	EW is Electronic Warfare, IAI is Israel Aerospace Industries Total UAVs is dataset: 273/Total Loitering Munitions: 37										

Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

Small loitering munitions can also be launched from vehicles or from larger flying devices. Developments add swarming capabilities for the control of multiple loitering munitions, such as Raytheon's Coyote, which combines different payloads into a single swarm system.[23] Israel is the leading developer and producer of loitering munitions, with 40 percent of the systems identified, with the United States and China following, both accounting for 12.5 percent. A prevalence of loitering munitions makes a new tactical modus operandi for ground troops necessary because the use of these UAVs affects the security of firing from cover.

Large Rotor-Based Platforms

Large rotor-based platforms include multi-rotor and mini-helicopter design features. Sixty percent of this segment is weaponized. China is the leading developer of the small helicopter design, offering missile launcher, machine gun, and small precision bomb capabilities. The Norinco Skysaker H300 and Ziyan Blowfish are examples.[24] Such systems are attractive alternatives for developing world armed forces seeking inexpensive close air support. China markets these systems to African and Middle Eastern countries.

Table 7. Large Rotor-Based Platforms

Purpose
Intelligence, Surveillance, Reconnaissance (ISR): 20%
Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR): 10%
Weapons Systems: 60% (Small missiles, Machine Guns, Grenades)

	Total (273)	Weaponized	Unarmed	ISR	ISTAR	EW	Relevant AI	Sector Specific Factors	Top Companies	Producer Countries (share of global total)	Operator
Rotor-based Large Developed	20	12 60% Armor Piercing: 9 (45%)	8 40%	4 20%	2 10%	1 5%	Autonomous mission capacity: 5 (25%) ATOL: 5 (25%) Teaming/ Swarming: 4 (20%) Auto in air replacement: 1 Fully autonomous combat capability: 1	Mini-Helicopter: 12 (60%) Multirotor: 8 (40%)	Norinco Ziyan Northrop Grumman	China: 7 (35%) USA: 3 (15%)	Navy Army/ Marines: Platoons
Rotor-based Large In Dev	2	1 50%	1 50%	1 50%				Mini-Helicopter: 1 Multirotor: 1			Navy Army/ Marines: Platoons
	EW is Electronic Warfare, ATOL is Automatic Take-Off and Landing Total UAVs is dataset: 273/Total Rotor-based platform: 22										

Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

Small Rotor-Based Platforms

Small rotor-based platforms are widely available in the commercial sector with advanced automation and video feed capabilities. In the military setting, small multi-rotors have the advantage of being an inexpensive option to provide localized situational awareness. The capability of such systems to carry a variety of sensor payloads that transmit to ground operators offers a variety of benefits. Such systems can be "tethered" to a power source to provide persistent ISR and grouped together as a swarm to provide perimeter defense. Importantly, they can autonomously conduct mapping operations in global positioning system (GPS)-denied environments. Exyn Technologies and Shield AI offer swarming multi-rotor systems to create maps in GPS-denied environments. The palm-sized Flir Black Hornet is equipped with thermal video and electro-optical capabilities for short range reconnaissance missions and has recently been deployed with the 82nd Airborne Division for use in Afghanistan.[25]

The weaponization of small multi-rotor platforms that can deploy payloads from the platform is a recent development and provides advantage over loitering munitions in that the platform itself is not destroyed in a given attack. The Australian company Skyborne released the Cerberus in 2019, a 6-kilogram platform capable of carrying payloads of miniature missiles, grenade launchers, or shotgun attachments.[26] South Africa's Rippel and the United Arab Emirate's Golden Group have collaborated to produce a small grenade launcher add-on that could be attached to existing small UAVs.[27] A

Table 8. Small Rotor-Based Platforms

Purpose
Intelligence, Surveillance, Reconnaissance (ISR): 83%
Weaponized: 10% (Small missiles, shotguns, Grenade Launchers)

	Total (273)	Weaponized	Unarmed	ISR	ISTAR	EW	Relevant AI	Sector Specific Factors	Top Companies	Producer Countries (share of global total)	Operator
Rotor-based small Developed	37	4	33	31 SSR: 22 83%	0	0	Percent: 6 (16%) Machine Vision: 5 (13.5%) Edge-AI: 4 (10%) Automated Perimeter detection: 2 Swarming: 1	IED detection: 1 Mapping: 1+	FLIR: 3 Elbit: 3 Aeraccess (France): 3	USA: 19 (51%) France: 7 (18%) Israel: 7 (18%)	Army/ Marines: Squads
Rotor-based small In Dev	2	0	2 100%	2 SSR: 22 60%			Autonomous image detection and classification: 1 (50%)	Self-charging UAV			Army/ Marines: Squads
	EW is Electronic Warfare, SSR is Surveillance Short Range Total UAVs is dataset: 273/Total Small Rotor-based platform: 39										

Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

flamethrower attachment has also been developed for the agricultural sector, which demonstrates a potential weapon system.[28]

Cargo and Transport UAVs

China's Tengdoen Technology is developing a 22-ton unmanned cargo plane, and the refitting of cargo helicopters with very simple remote-control interfaces has been demonstrated in the United States.[29] Smaller UAVs can make precision cargo drops, and glider UAVs can be launched from airplanes.[30] The military logistics implications of automated aerial cargo transfers are significant.

The potential of automated transport is shown in the commercial sector, with China's Ehang developing a "low altitude aerial vehicle" and the U.S. Kittyhawk pursuing a similar project that received funding from the Defense Innovation Unit.[31] While these are essentially "manned," the control interface is that of a simple UAV, as most of the flying processes are automated. While not military projects, these deserve mention because of the ease of adaptation of such systems for military purposes. Commercial non-military urban air mobility is the focus of enormous investment and clearly of significance in technological advances relevant to UAV development.[32]

AI in UAVs

The following sections focus on the key areas of AI relevant for UAVs and demonstrate their combined potential force multiplier effect. In the dataset analyzed, the following broad areas of application of AI in UAVs were found: air combat, machine vision, teaming, auto mission, swarming, and auto-flight. Figure 2 offers an indicator of the different instances where AI breakthroughs and UAVs crossover.

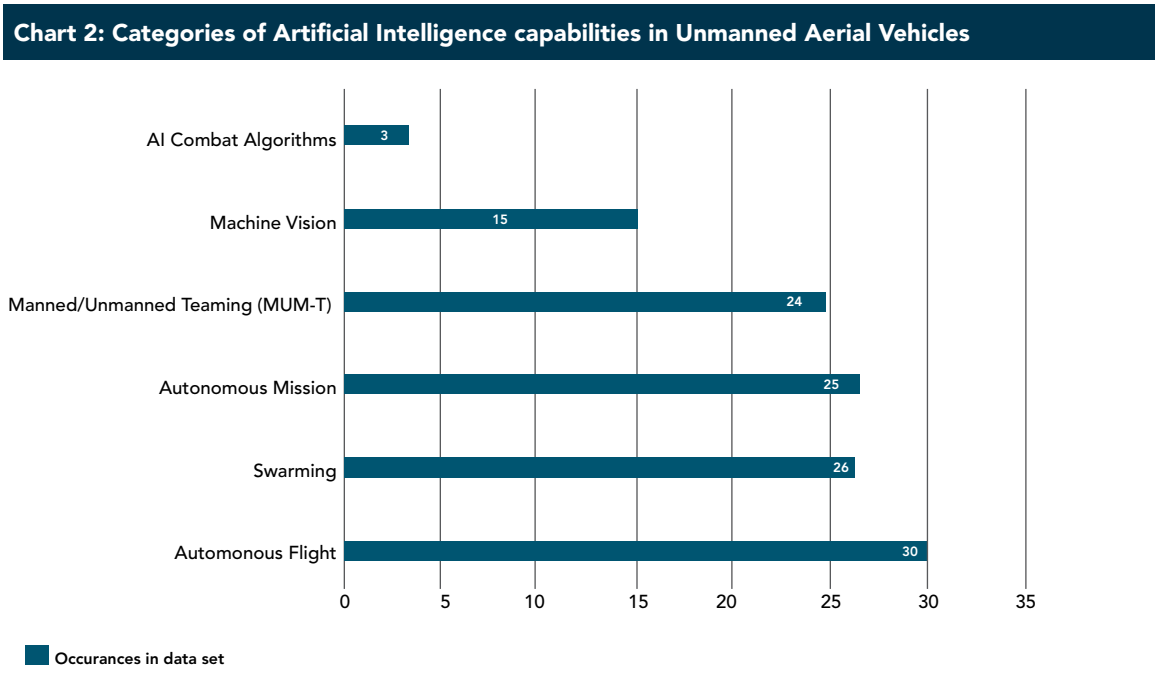
Table 9. Cargo and Transport UAVs

Purpose
Transport and Cargo delivery
Weaponized: 0%

	Total (273)	Weaponized	Unarmed	ISR	ISTAR	EW	Relevant AI	Sector Specific Factors	Top Companies	Producer Countries (share of global total)	Operator
Cargo & Transportation Developed	8	0	8				ATOL: 1 (12.5%)	V. Heavy (1.5 tons): 1 China Medium Heavy: 2 Light: 6	Star UAV Sunhawk	USA: 19 (51%) France: 7 (18%) Israel: 7 (18%)	China: 2 (25%)
Cargo & Transportation In Dev	10						ATOL: 4 (40%)	V. Heavy (22 tons): 1 China Passenger transport: 6 Helicopter re-fit: 3 Glider: 2	Ehang Kittyhawk Lockheed Martin	USA: 7 (70%) China: 2 (20%)	
	Total UAVs is dataset: 273/Total Cargo & Transport UAVs: 18										

Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

Figure 2. Artifical Intelligence in UAVs



Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

Air Combat Algorithms

Air combat algorithms have shown success in the combat simulator environment, as demonstrated by Psibernetix and the Air Force Research Laboratory (AFRL) in 2016 using "Genetic Fuzzy Trees" neural networks.[33] The advantage of such a system is that experienced human pilots can teach the AI system in an intuitive way. The Defense Advanced Research Projects Agency (DARPA) Air Combat Evolution program has created a competitive environment for AI developers to automate air-to-air combat, and AFRL and Lockheed Martin Skunk Works conducted a series of tests in 2017 that successfully demonstrated algorithmic control of an unmanned F-16 in an air-to-ground strike mission while adapting to complex challenges.[34]

Machine Vision

Machine vision refers to the automated classification of labelled data within a visual format.[35] It provides situational awareness capacity, such as object detection and classification, and when applied to multi-sensor fusion can detect and track in obscured environments, as well as being used for targeting purposes. Machine vision is also essential for vision-based navigation.

Certain aspects of machine vision are suited to smaller UAVs because of the close proximity to targets or the small areas they can survey. At this level, facial recognition, gait recognition, or reading license plates is possible. A tactical example for the use of machine vision was an urban combat exercise conducted in 2017 that utilized a thermal camera mounted on a small multi-rotor

UAV linked to a machine vision processing application. The system was able to identify a concealed sniper waiting in ambush and to advise the team of the threat.[36]

The integration of AI allows for the automated classification of sensor information in general. AI can process electro-optical sensor data for increased accuracy in targeting.[37] Synthetic aperture radar sensors can be empowered by AI for automated target recognition and tracking.[38] Lidar sensors combined with AI and mounted on small UAVs can quickly produce three-dimensional maps and identify hidden structures or find safe landing areas.[39] Also related to machine vision are the other areas of AI and sensor fusion that, when used together, can significantly enhance UAV detection capabilities to provide more accurate situational awareness.

Manned-Unmanned Teaming (MUM-T)

MUM-T has been recognized as a strategic priority for the three branches of the military for force multiplication, allowing individual warfighters to work as part of a collaborative network with unmanned aerial systems and allowing a single user to team with unmanned vehicles.

At the Air Force level, UCAV development is focused on creating "Loyal Wingmen;" using simple and intuitive interfaces, individual pilots will team with accompanying unmanned aircraft capable of autonomous decisionmaking to achieve strategic objectives. The lead Air Force project under way in 2019 is the "Skyborg," in which a pilot functions like a "quarterback in the sky that's working with a team that can call audibles and change what they do."[40]

This concept is a global trend and runs through current allied development projects such as Boeing's Air Force Teaming project in Australia, Europe's Future Combat Air System, and BAE's Taranis UCAV project. Ma Hongzhong, chief engineer of China Aerospace Science and Industry Corporation, explained that their Skyhawk Stealth UCAV has manned-unmanned capacity, and the Russian Sukhoi UCAV project has an emblem of a UCAV linked to a fighter jet on its tail, strongly suggesting it is also a MUM-T project.[41]

The Army has demonstrated MUM-T in attack helicopters teamed with Grey Eagle MALE UAVs or tactical UAVs such as the RQ-7 Shadow since 2014, with the purpose of extending controller range into contested environments, scouting, and conducting attacks beyond the line of sight.[42]

At the ground level, the Army vision for Manned/Unmanned teaming states that "autonomous unmanned systems will function as members of the formation executing tasks as well as providing oversight for subordinate systems. This capability will allow leaders to employ unmanned systems for critical and complex tasks such as establishing a mesh communication network or reconnoitering and mapping subterranean infrastructures."[43]

Automated Missions

The loitering munitions segment has UAVs available that can autonomously strike given targets using machine vision. A variety of Israeli and Turkish loitering munitions have autonomous capabilities, as the UAV can identify relevant targets that have been preapproved for strike. Chinese mini-helicopters available from Ziyan and Norinco can be preprogrammed to strike selected targets or conduct mission commands.[44] Autonomous cargo delivery is also a growing area of interest, with refitted helicopters being controlled by infantry on tablet interfaces.[45] In contested electromagnetic environments, preprogramming strike and ISR are viable strategies. As AI develops, AI-enabled UAVs will be able to perform more complex commands and behaviors.

Swarm of security drones with surveillance camera flying in the sky. 3D rendering image

Swarming

As General John Allen noted in 2017,

> *Here is where semi and autonomous systems are very important for us—re: a near-peer competition who has invested a lot in autonomous systems, and at a tactical or operational level you are going to have to deal with swarm after swarm of intelligent robots who not only have been trained to locate your position via virtue of your [electromagnetic] signature, but also facial recognition, recognizing flaws and weaknesses in defenses and jamming cyber, and worst, all cooperating with each other.*[46]

Swarming is a key area for AI and UAV development, requiring leveraging artificial intelligence for the calibration of swarm movements and tactics toward a given objective. Swarms are usually composed of small multirotor UAVs, mini-helicopters, or tube-launched loitering munition type devices with

heterogenous capabilities, such as ISR, electronic warfare (EW), or munitions payloads as seen in Raytheon's Coyote.[47]

Many research projects have been developed for the air launch of swarms of small UAVs. Kratos and AeroVironment have signed a cooperation agreement to pair the Kratos attritable UTAP-Mako UCAV with AeroVironment's Switchblade loitering munitions.[48] MBDA Missile Systems has developed a glider missile carrier that can release small UAVs in a similar manner.[49] Such systems show potential for denied airspace where communication is not possible. DARPA's Collaborative Operations in Denied Environments project is researching how teamed UAV systems could collaborate autonomously with each other for three-dimensional targeting in denied airspace for strike purposes.[50] The U.S. Air Force Research Lab and India have established a cooperation agreement for research into air-launched swarm systems.[51] During the 2019 Mad Scientist workshop, former Deputy Secretary of Defense Robert Work suggested that a possible strategy for swarms would be to launch them in carrier projectiles from long-range artillery guns, an interesting idea for denied area penetration.[52]

At the ground level the challenge is to develop a system where the swarming missions of multi-rotor UAVs can be coordinated via a simple interface. DARPA is working on this capability under project OFFset—Offensive Swarm Enabled Tactics.[53]

Russia is developing swarm capabilities in the form of small multi-rotor UAVs equipped with explosive devices, nicknamed "*Jihadi Aviation*."[54] China is the current record holder for the largest drone swarm demonstration involving 119 small fixed-wing UAVs.[55] Mini-helicopter UAV manufacturers Norinco and Ziyan have demonstrated swarm tactics with mini-helicopters.[56]

The economical price of small loitering munitions and small multi-rotor UAVs make them relevant for force multiplication and situations where the chances of the UAV being destroyed or lost are high. The capacity for swarms to use local sensors to coordinate with each other and operate autonomously also makes them suited for contested environments. The usefulness of the UAVs depends on the AI software controlling them which, once developed, should not affect the overall production cost of such units.

The tactical possibilities of swarms with heterogenous payloads, sensors, and strike capabilities require creativity and the testing of such systems in war-game scenarios to assess their functionality.[57] A multinational exercise involving teaming ground units coordinating swarms of multi-rotor UAVs in a "Contested Urban Environment" was demonstrated in Canada in 2019. The swarm provided improved situational awareness, generated three-dimensional maps of the interiors of buildings and was able to drop ground sensors.[58]

Autonomous Flight

In current systems, the potentially dangerous take-off and landing phases even of large UAVs have been increasingly automated and are made easier with VTOL-capable platforms. The development of automated flight is important for missions in contested airspace where a remote-control link is not possible.

Contested airspaces pose a challenge, as UAVs can be detected when emitting radio frequency transmissions, as well as operational failure in electromagnetic vacuums where GPS navigation is not possible. Cognitive visual navigation and image mosaicing are research areas where visual data and onboard AI processing are leveraged for autonomous navigation.[59] For small UAVs, autonomous flight is being explored with machine vision algorithms to scan and avoid obstacles.

Counter-UAV Systems

High-powered laser defense systems for UAVs have been developed by China, Israel, and the United States, and high-powered microwave deterrence

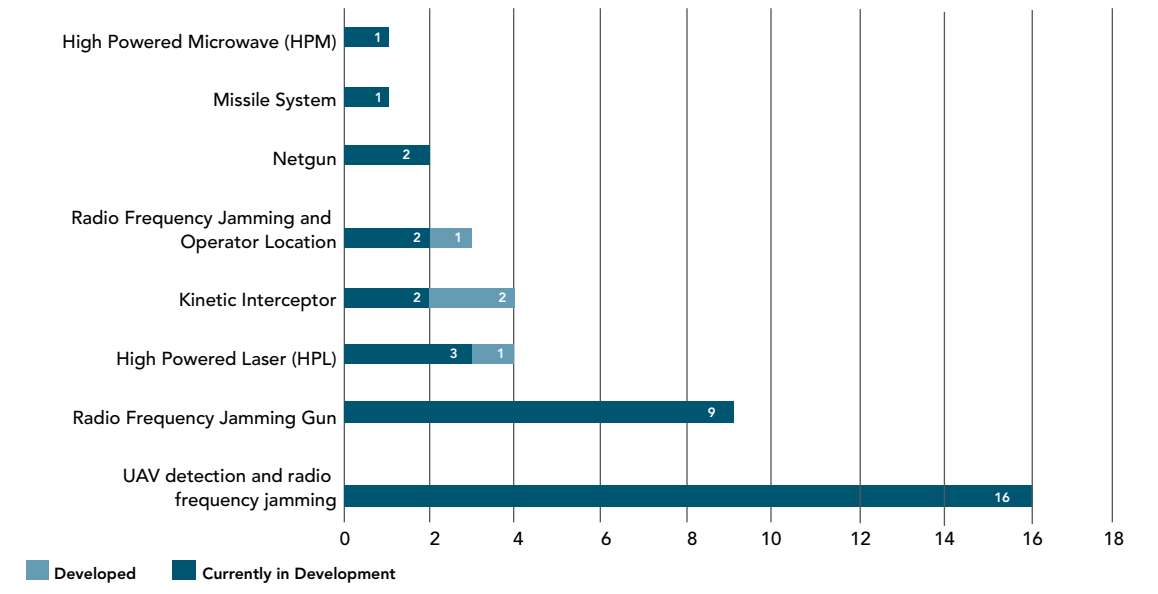
systems are in development by the U.S. Army and Air Force.[60] Artificial intelligence is well integrated into counter-UAV systems in areas such as multi-sensor fusion, algorithmic radio frequency analysis, automated visual recognition, and pixel analysis, to name a few. Figure 3 offers a breakdown of counter-UAV systems identified.

AI and Electronic Warfare Systems for UAVs

Regarding UAVs as electronic warfare devices, radar systems can be empowered by AI to detect and mitigate threats through calculated frequency alterations, allowing for cognitive electronic warfare.[61] Machine-learning applied to radio frequencies (RFs) can automate classification of objects. A demonstration in Turkey showed multiple UAVs used to triangulate and accurately locate the operator of an RF signal.[62] Quantum radar is a growing area of interest for lowering the chances of control and communication interception; however, this research is still in the initial stages of development.[63]

Russia has advanced capabilities in this area, as demonstrated in Syria, Ukraine, and the Arctic region.[64] A counter-UAS system revealed in June 2019 creates "vacuum" spaces against aerial threats using a three-pronged approach of linked ground systems. The RB-301B Borisoglebsk targets ground-to-airborne communications, the Krasukha system jams airborne radars and AWACS signals, while the Zhitel system interferes with satellite navigation systems and mobile phone connections.[65] Russia also claims to have set up "an EW shield" along the Arctic coast capable of jamming satellite and drone communications, GPS signals, and other navigational system at ranges of up to 5,000 and 8,000 kilometers.[66] China has made unconfirmed claims

Figure 3. Counter-Unmanned Aerial Vehicle Systems



Source: UAV technical specifications complied by the authors between February and August 2019. Specifications for each UAV system gathered from manufacturer web sites and specialist UAV news web sites are listed in note 7.

to have developed "quantum radar technology" to detect stealth aircraft.[67] A long-range quantum-secured communication network between Beijing and Shanghai was demonstrated in 2017.[68] China's electronic warfare has been outlined by the U.S. Army Training and Doctrine Command:

> *The Chinese strategy, known as integrated network electronic warfare, combines EW, computer network operations, and nonlethal strikes to disrupt battlefield information systems that support an adversary's warfighting and power-projection capabilities.*[69]

The current battle network strategy for incorporating the force multiplication benefits of UAV situational awareness, exciting as they are, has emerged from an asymmetrical warfare context. Syria provided a first taste of new contested environments where there were setbacks as a consequence of Russian electronic warfare attacks.[70] Electronic warfare to disrupt a near-peer's manned/unmanned situational awareness and strike capability must be prioritized.

Creativity and applied cutting-edge research are needed to conceptualize a linked battle network of manned and unmanned systems. Wireless data transfer, GPS, and RF communications will be limited, and a sufficiently adaptive system will be necessary.[71] In addition, the challenge of advanced situational awareness capabilities from AI-empowered sensor networks offers challenges for the movement of persons and vehicles.

According to T.X. Hammes, at the operational level the fielding of advanced unmanned systems in a contested battle environment will lead to defensive tactics dominating battlefields where unmanned systems are prevalent. If any individual or vehicle creates a signature, it can be seen and attacked. Neither side will be able to maneuver freely. In Hammes's analysis, this offers the North Atlantic Treaty Organization (NATO) a strategic advantage in relation to the threat of Russian incursions into NATO-held territory.[72] This change in the character of war applies to any space where the technology of capable peers may be involved.

The prioritization of UAV platform acquisition and battle network development should be informed by these caveats. For such environments, Edge-AI, machine learning for vision-based navigation, and autonomous mission capabilities should be prioritized, as well as a battle network and modus operandi that require minimal data transfers.

A reorientation of the battle network for manned/unmanned integration toward highly contested electromagnetic environments should be a priority for UAV platform and battle network development goals and requirements, in order to offset the situational awareness and electronic warfare capabilities of competitors.

Coping with the Competition

This article has focused on the different types of unmanned aerial platforms, AI use cases, and development areas, as well as considerations for the future operating environment. We aim to have given the reader insight into the different elements of AI relating to unmanned systems through concrete and operational use case examples to provide an informed understanding of the manned and unmanned aerial potential available. This information can be used to understand and predict China's tactical use of AI and to identify and prioritize research areas of systems in the near-peer competition context.

Near-peer competition is the focus of the U.S. National Defense Strategy of 2018, which demands a coherent response and an adequate assessment of near-peer technological innovation trajectories. Within the specific platforms, China has an edge in AWACS-enabled platforms, an unknown capacity in UCAV platforms, a competitive MALE platform development market, and advanced mini-helicopter use. A greater challenge is China's integration of the systems approach designed to share information, such

as the Strategic Support Force, established in 2015, which organizes space, cyber, intelligence, surveillance, and reconnaissance in the same command. The United States does not yet have equivalent integration.[73] China is actively pursuing the integration and widespread military adoption of AI, as part of its civil-military fusion approach. In addition, an Intelligent Unmanned Systems and Systems of Systems Science and Technology Domain Expert Group has been set up within the Peoples' Liberation Army.[74]

China's successful export-oriented approach to developing MALE UAVs suggests a wider impact of such technologies around the world and entrenches a dependence on Chinese operating systems among buyers.[75] China's Global Navigation Satellite System, *Beidou*, which aims to have total global coverage in 2020 as well as global communication infrastructure development, adds to an environment that enables China's force projection potential using a manned/unmanned strategy.[76]

China has demonstrated capability in appropriating advanced research and technology from around the world, translating this into its own military UAV platforms. It is the AI inside such systems that will be a key differential in the hyperwar context.[77] China is actively pursuing swarming capabilities, manned/unmanned teaming, and AI-enabled multi-sensor fusion, for example. China's track record of translating scientific research into military capabilities via civil-military fusion is proven.[78]

Based on the data presented in this article, the authors recommend an approach built on the combination of a centralized AI core and a decentralized AI nervous system inside the military and intelligence architectures. "Multidomain warfare involves colossal amounts of heterogenous data streams that can be exploited only with the help of AI. While the ability to manage this data colossus in real time promises tremendous advantages, failure to draw meaning from that information could spell disaster."[79]

UAVs are sensing organs that receive information from the external world. Currently, AI is moving forward on individual platforms; however, a centralized situational awareness AI core and a decentralized AI nervous system are required to synchronize and aggregate the overwhelming amount of sensor data necessary. A shift in thinking from a platform-centric approach to one creating the core architecture to syndicate such systems is essential:

> *AI-supported weapons, platforms, and operating systems rely on custom-built software and hardware that is specifically designed for each separate system and purpose. There is currently no master mechanism to integrate the scores of AI-powered systems operating on multiple platforms.*[80]

This AI core and nervous system priority must be part of both short-term and long-term planning, in recognition of its force multiplication potential. It also must be considered as a key element of any manned/unmanned strategy, to avoid being offset by a more AI-empowered and -integrated competitor. The AI core and AI nervous system must be recognized as a strategic necessity, be part of urgent short-term planning, inserted into all medium-term and long-term planning as the highest priority, and properly financed in budgetary allocations.

A second recommendation is to develop AI "horizontal open innovation coalitions." The AI research community is open and global, a horizontal open innovation ecosystem. The commercial sector operates with freedom of transit oriented by the principle goal of increasing profit, rather than matters of national security. The fruits of this garden are there for the taking, alongside the danger of the most advanced AI technology being offered up to military competitors. Such a reality requires a dramatic refocusing of resources to transfer relevant insight and technology toward strategic goals.

Understanding this dynamic necessitates a proactive approach to scout and recruit technological and scientific advances that translate into asymmetric advantages faster than China or Russia, as well as the creation of mechanisms to apply this advanced research to an ecosystem of relevant traditional and newly emerging AI-focused manufacturers and contractors.

Significant Intelligence Community–led industrial innovation research into applied artificial intelligence is imperative. This suggests an expanded global role for the institution of the Defense Innovation Unit, made actionable by informing the actions of a specially created funding framework for applied AI and innovation partnerships *globally*, including "tech scouting."

For technology laggards to compete with a more powerful competitor, they must establish horizontal open collaboration coalitions. This was the successful strategy used by General Motors, Daimler, Chrysler, and BMW, who formed a "Global Hybrid Alliance" in the face of superior technology and market share of Toyota. It was only by working together, pooling research and development capabilities, that they were able to rebound.[81]

The creation of such a horizontal open innovation coalition for defense AI is required to establish mutually beneficial technology investment partnerships among allied countries facing the threat of China's ascendance. This would require pooling intellectual, engineering, and financial capabilities from among allies in NATO, giving the institution a new raison d'être and maximizing the potential of their respective AI endeavors. In addition, alliances with Israel, Australia, South Korea, Japan, and India should be fostered to co-develop applied artificial intelligence for the unmanned defense industry capacity. NATO Allied Command Transformation Deputy Chief of Staff Lieutenant General Thomas Sharpy, USAF expressed the potential for the alliance to capitalize on synergies between member nations toward developing preparedness through enhanced cooperation:

> *One of the things that I see is the power of the alliance of 29 nations—this brings with it the intellectual capacity and the investment by the 29 nations, the leadership of 29, and the academic institutions and diversity of thought that 29 bring. It's an amazing opportunity for us to take all of that, synchronize it, consolidate it, and use it to figure out how we can be better, more effective, more efficient, and I think be a stronger deterrent for any potential adversary to think twice before they act.*[82]

A recent Defense Technology and Trade Initiative (DTTI) between the Air Force Research Laboratory and India's Defence Research and Development Organization to collaborate on a UAV swarm development program appears to be an example of a step in the right direction.[83] The DTTI states that it seeks to move "away from the traditional 'buyer-seller' dynamic toward a more collaborative approach and explore new areas of technological collaboration from science and technology cooperation through co-development and co-production."[84] Another relevant example is Softbank's Vision Funds. The first is valued at $100 billion and invests in artificial intelligence with contributions from Saudi Arabia's Public Investment Fund and the United Arab Emirates' sovereign wealth fund. Vision Fund Two also invests in artificial intelligence and is a $108 billion fund, with contributions from Kazakhstan's sovereign wealth fund and Microsoft.[85]

Such a plan requires a new form of cooperation and coordination between diplomatic and trade departments, the scientific community, defense equipment manufacturers, and outreach to the commercial sector, Intelligence Community, and defense institutions. While there are inherent risks involved in this approach, such alliances would be not only

mutually beneficial but also are essential in the face of an ascendant China with a growing defense alliance with Russia. As senior defense thinkers have stated, risks must be taken in order to avoid the predictable failure of the path dependency based on a conservative and risk-averse culture.[86]

Killing Me Softly

Through quiet and steady innovation and expansion of their military topography, China is achieving a "killing me softly" impact on U.S. military capabilities. The danger of remaining laggards is illustrated by this examination of UAV technology and AI adaptations. We must be vigilant on all frontiers—not only those outlined by our geographies, but also the new frontiers created by advancements in technology and science.

We lift our eyes to the larger context of AI and the global military landscape where there are important calls for AI in weapons systems that could enable automated strikes to be regulated by international treaty, as proposed by Douglas Frantz, former Deputy Secretary-General of the Organisation for Economic Co-operation and Development:

> *Standards should be set for monitoring AI systems. Fundamental human rights should be specifically protected. A new international body should be created for oversight, similar to the International Atomic Energy Agency. AI is technology that must be controlled. The world reached a consensus in the 1960s and reined in an existential risk. It can be done again.*[87]

In the absence of such limiting international accords, we find ourselves in a contest for the future—a contest we must win. PRISM

Notes

[1] Frank G. Hoffman, "Will War's Nature Change in the Seventh Military Revolution?" *Parameters* 47, no. 4 (2017): 19–31, available at <https://ssi.armywarcollege.edu/pubs/parameters/issues/Winter_2017-18/5_Hoffman.pdf>.

[2] Field Cady and Oren Etzioni, "China May Overtake US in AI Research," Allen Institute for Artificial Intelligence, March 13, 2019, available at <https://medium.com/ai2-blog/china-to-overtake-us-in-ai-research-8b6b1fe30595>; Elsa Kania, "The Dual-Use Dilemma in China's New AI Plan: Leveraging Foreign Innovation Resources and Military-Civil Fusion," Lawfare, July 28, 2017, available at <https://www.lawfareblog.com/dual-use-dilemma-chinas-new-ai-plan-leveraging-foreign-innovation-resources-and-military-civil>.

[3] Christine Fair, "Pakistan's Army Is Building an Arsenal of 'Tiny' Nuclear Weapons—And It's Going to Backfire," *Quartz India*, December 22, 2015, available at <https://qz.com/india/579334/pakistans-army-is-building-an-arsenal-of-tiny-nuclear-weapons-and-its-going-to-backfire/>.

[4] Surana Praggya, "BeiDou & A2AD: Where is China Headed?" *Indian Defense Review*, March 13, 2017, available at <http://www.indiandefencereview.com/spotlights/beidou-a2ad-where-is-china-headed/>.

[5] Nick Heath, "What Is Artificial General Intelligence?" *ZNET*, August 22, 2018, available at <https://www.zdnet.com/article/what-is-artificial-general-intelligence/>; David Senior, "Narrow AI: Automating the Future of Information Retrieval," *Techcrunch*, January 2015, available at <https://techcrunch.com/2015/01/31/narrow-ai-cant-do-that-or-can-it/>.

[6] Tony Thomas, "The Battle with China for Military Technological Superiority," Aspen Security Forum, July 20, 2019, available at <https://www.youtube.com/watch?v=htNYoNhjiHk>.

[7] Original research conducted by George Howell between February and August 2019, for forthcoming RAIN Research report. Specifications for each UAV system gathered from manufacturer websites and specialist UAV news websites including: *Jane's Defense Weekly*, <https://www.janes.com>; UAS Vision global news service, <http://www.uasvision.com/>; *UAS Weekly*, <www.uasweekly.com>; C4ISR.net, <https://www.c4isrnet.com/unmanned/>; Israel Homeland Security, < https://i-hls.com/>; Military Factory™, <https://www.militaryfactory.com/aircraft/unmanned-aerial-vehicle-uav.asp>; Defense Systems, <https://defensesystems.com/pages/topics/unmanned-systems.aspx>; and Unmanned Systems Technology, <https://www.unmannedsystemstechnology.com/category/news/uav-news/>.

[8] U.S. Army, *U.S. Army Unmanned Aircraft Systems Roadmap 2010–2035: Eyes of the Army* (Fort Rucker, AL: UAS Center of Excellence, April 9, 2010), available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/a518437.pdf>.

[9] Global Data, *Global Military UAV Market 2018–2028*, May 2018, available at <https://www.reportlinker.com/p05466933/Global-Military-UAV-Market.html>.

[10] Tegg Westbrook, "The Global Positioning System and Military Jamming: Geographies of Electronic Warfare," *Journal of Strategic Security* 12, no. 2 (2019): 1–16, available at <https://doi.org/10.5038/1944-0472.12.2.1720>.

[11] Ron Ben-Yishai, "The Race Is on to Retrieve the U.S. Spy Drone Brought Down by Iran," *Ynet News*, June 6, 2019, available at <https://www.ynetnews.com/articles/0,7340,L-5529508,00.html>.

[12] Jeremy Binnie, "Global Hawk Shootdown Validates Iran's Indigenous SAM Capabilities," *Jane's 360*, June 21, 2019, available at <https://www.janes.com/article/89422/global-hawk-shootdown-validates-iran-s-indigenous-sam-capabilities>.

[13] Shishir Gupta, "India Rethinks Buying U.S. Armed Drones," *Hindustan Times*, July 28, 2019, available at <https://www.hindustantimes.com/india-news/india-rethinks-buying-us-drones/story-lrXANhzediWzKLd6j9bsqJ.html>.

[14] International Defence Security and Techology, "Reaper and Global Hawks Being Modernised to Defeat A2/AD Environment Through Longrun High Resolution Sensing and Cybersecurity," July 25, 2019, available at <https://idstch.com/reaper-global-hawks-defeat-a2-ad-environment-employing-long-range-high-resolution-sensors/>; Chad Garland, "Iran Attack Was First Successful Takedown of a Global Hawk Drone," *War is Boring*, June 21, 2019, available at <warisboring.com/iran-attack-was-first-successful-takedown-of-a-global-hawk-drone/>.

[15] Jeffrey Lin, and P. W. Singer, "China's New Drone Company Is Building a UAV with a 20-Ton Payload," *Popular Science*, January 23, 2018, available at <https://www.popsci.com/chinas-new-drone-company-has-big-plans/#page-3>.

[16] Lin Xieyi, "How Capable Is Chinese AWACS as Compared to U.S. or Israeli systems?" Quora, July 17, 2017, available at <https://www.quora.com/How-capable-is-Chinese-AWACS-system-as-compared-to-US-or-Israeli-systems>; "Divine Eagle: China's Massive New Drone Designed to Seek and Destroy F-35s," *Military Watch Magazine*, June 2, 2019, available at <https://militarywatchmagazine.com/article/divine-eagle-china-s-massive-new-drone-designed-to-seek-and-destroy-f-35s>.

[17] David Axe "China's Giant Spy Drone Just Tailed a U.S. Navy Cruiser." *Yahoo News*, July 19, 2019, available at <https://news.yahoo.com/china-giant-spy-drone-just-072700604.html>.

[18] Minnie Chan, "Chinese Drone Factory in Saudi Arabia First in Middle East," *South China Morning Post*, March 26, 2017, available at <https://www.scmp.com/news/china/diplomacy-defence/article/2081869/chinese-drone-factory-saudi-arabia-first-middle-east>.

[19] David Donald, "AEW Goes Unmanned," *Jane's 360*, February 19, 2019, available at <https://www.janes.com/article/86563/aew-goes-unmanned-idex19d3>.

[20] Stockholm International Peace Research Institute, "SIPRI Arms Transfers Database," 2019, available at <https://www.sipri.org/databases/armstransfers>.

[21] "Autonomous Device Experts," ADE, 2017, available at <http://www.adeinc.io/eng/index.html>; Aeronautics, "Homeland & Security," *Aeronautics*, 2019, available at <https://aeronautics-sys.com/>.

[22] David Oliver, "MBDA Reveals Spectre UAV,"*Armada International*, September 26, 2018, available at <https://armadainternational.com/2018/09/mbda-reveals-spectre-uav>.

[23] Raytheon, "Mind of the Swarm," June 29, 2018, available at <https://www.raytheon.com/news/feature/mind-swarm>.

[24] I-HLS, "Sky Saker—China's New Armed Unmanned Helicopter," March 26, 2016, available at <https://i-hls.com/archives/68931>; Richard Fisher, Jr., "AAD 2018: China's Blowfish I VTOL UAV Enters Service with PLAN," *Jane's Defense Weekly*, September 21, 2018, available at <https://www.janes.com/article/83264/aad-2018-china-s-blowfish-i-vtol-uav-enters-service-with-plan>.

[25] Exyn, "Powering Aerial Autonomy," available at <https://www.exyn.com/>; Shield AI, "Artificial Intelligence for a Safer More Secure World," available at <https://www.shield.ai/>; Flir System. Inc., "Black Hornet PRS," available at <https://www.flir.com/products/black-hornet-prs/>; Andrew Liptak, "U.S. Troops in Afghanistan Will Soon Test a Tiny, Pocket-Sized Drone in the Field," *The Verge*, June 30, 2019, available at <://www.theverge.com/2019/6/30/20123805/us-army-82nd-airborne-division-flir-black-hornet-personal-reconnaissance-drone-afghanistan>.

[26] Skyborne, "Cerberus GL," available at <https://skybornetech.com/cerberus-gl>.

[27] Sam J. Basch,"Grenades Launched from Light UAVs," *Jane's 360*, February 19, 2019, available at <https://www.janes.com/article/86547/grenades-launched-from-light-uavs-idex19d3>.

[28] João Antunes, "How Can a Flamethrower on a Drone be Utilized by Commercial UAS Operators?" *Expo UAV*, July 19, 2019, available at <https://www.expouav.com/news/latest/flamethrowers-drones/>.

[29] Jeffrey Lin and P.W. Singer, "China's New Drone

Company Is Building a UAV with a 20-Ton Payload," *Popular Science*, January 23, 2018, available at <https://www.popsci.com/chinas-new-drone-company-has-big-plans/#page-3>; Justin Katz, "UAV Autonomy Solution Spurs Marine Corps to 'Cross Bins' with Mission Sets," *Inside Defense*, December 14, 2017, available at <https://insidedefense.com/daily-news/uav-autonomy-solution-spurs-marine-corps-cross-bins-mission-sets>.

[30] Military Factory, "Yates Electrospace Silent Arrow," available at <https://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=1955& Bluebird Aero Systems>, and "Thunder B," available at <http://www.bluebird-uav.com/thunderb-2/>.

[31] Ehang, "Ehang AAV," available at <www.ehang.com/ehang184>; Mark Harris, "Ready for Liftoff? Two Flying Taxi Startups Got Pentagon Funding," *The Guardian*, July 10, 2019, available at <https://www.theguardian.com/technology/2018/jul/10/flying-cars-taxis-pentagon-us-military-funds-joby-kitty-hawk>.

[32] Morgan Stanley, "Urban Air Mobility Flying Cars: Investment Implications of Autonomous Urban Air Mobility," December 8, 2019.

[33] David Humbling, "AI Pilot Helps U.S. Air Force with Tactics in Simulated Operations," New Scientist, November 22, 2016, available at <https://www.newscientist.com/article/2113709-ai-pilot-helps-us-air-force-with-tactics-in-simulated-operations/>; Nicholas Ernest et al., "Genetic Fuzzy Based Artificial Intelligence for Unmanned Combat Aerial Vehicle Control in Simulated Air Combat Missions," *Journal of Defense Management* 6, no. 1 (2016), available at <https://www.researchgate.net/publication/301944635_Genetic_Fuzzy_based_Artificial_Intelligence_for_Unmanned_Combat_Aerial_Vehicle_Control_in_Simulated_Air_Combat_Missions>.

[34] Defense Advanced Research Projects Agency, "2019. Training AI to Win a Dogfight," May 8, 2019, available at <https://www.darpa.mil/news-events/2019-05-08>; Lockheed Martin, "U.S. Air Force, Lockheed Martin Demonstrate Manned/Unmanned Teaming," April 10, 2017, available at <https://news.lockheedmartin.com/2017-04-10-U-S-Air-Force-Lockheed-Martin-Demonstrate-Manned-Unmanned-Teaming>.

[35] Wikipedia, "Machine Vision," June 2, 2019, available at <https://en.wikipedia.org/wiki/Machine_vision>.

[36] "Unmanned Experts Joins Cogniac to Provide Live, Threat-Analyzed UAV Imaging to Army Battle Exercise Team," *UAS Weekly*, January 4, 2017, available at <https://uasweekly.com/2017/01/04/unmanned-experts-joins-cogniac-provide-live-threat-analyzed-uav-imaging-army-battle-exercise-team/>.

[37] Jong-hun Kim et al., "Development of an Electro-optical System for Small UAV," *Aerospace Science and Technology* 14, no. 7 (2010): 505–511, available at <https://www.sciencedirect.com/science/article/pii/S1270963810000404>.

[38] Ke Wang et al., "Aperture Radar Image Generation with Deep Generative Models," *IEEE Geoscience and Remote Sensing Letters* 16, no. 6 (2018); Feng Zuo et al., "Improved Method of Video Synthetic Aperture Radar Imaging Algorithm," *IEEE Geoscience and Remote Sensing Letters* 16, no. 6 (2018): 897–901, available at <https://ieeexplore.ieee.org/document/8580384>.

[39] Young Hoon Shin, Sunghwa Lee, and Jiwon Seo, "Autonomous Safe Landing-Area Determination for Rotorcraft UAVs Using Multiple IR-UWB Radars," *Aerospace Science and Technology* 69 (2017): 617–624, available at <https://www.sciencedirect.com/science/article/pii/S1270963817310568>.

[40] Sara Sirota, "Air Force Seeks 'Quarterback in the Sky' with Skyborg Program by 2023," *Inside Defense*, March 21, 2019, available at <https://insidedefense.com/daily-news/air-force-seeks-quarterback-sky-skyborg-program-2023>.

[41] Tom Dunlop, "New Chinese 'Sky Hawk' Stealth Drone in First Public Flight," *UK Defence Journal*, January 14. 2019, available at <https://ukdefencejournal.org.uk/new-chinese-sky-hawk-stealth-drone-in-first-public-flight/>; YouTube, "Russia's Secret Sukhoi Su-70 Attack Drone 'Okhotnik-B' Prototype of 6th Gen Stealth Fighter," January 24, 2019, available at <https://www.youtube.com/watch?v=7zIG_8-IQW0>.

[42] Mark Pomerleau, "Army's Multidomain Battle Brings Manned-Unmanned Teaming to the Fore," *C4ISRNET*, August 31, 2017, available at <https://www.c4isrnet.com/unmanned/uas/2017/08/31/armys-multidomain-battle-brings-manned-unmanned-teaming-to-the-fore/>.

[43] TRADOC Pamphlet 523-3-6, "The U.S. Army Functional Concept for Movement and Maneuver," February 2017, available at <https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-6.pdf>.

[44] AZO Robotics, "Ziyan UAV's Unmanned Helicopter Set to Redefine Aerial Logistic Platform," July 13, 2016, available at <https://www.azorobotics.com/News.aspx?newsID=8618>; iHLS, "Sky Saker—China's New Armed Unmanned Helicopter."

[45] Justin Katz, "UAV Autonomy Solution Spurs Marine Corps to 'Cross Bins' with Mission Sets," *Inside Defense*, December 14, 2017, available at <https://insidedefense.com/daily-news/uav-autonomy-solution-spurs-marine-corps-cross-bins-mission-sets>.

[46] John Allen, "Hyperwar," Sparkcognition Time Machine Conference, November 13,

2017, available at <https://timemachine.ai/tm2017-sessions/#watch-FqHQj9A5oGoursujAB8uBk>.

[47] Raytheon, "Coyote UAS," available at <https://www.raytheon.com/capabilities/products/coyote>.

[48] Kelsey Atherton, "Smart Drones to Command and Launch Smarter Missiles," *C4ISRNET*, May 8, 2019, available at <https://www.c4isrnet.com/unmanned/2019/05/08/smart-drones-to-command-and-launch-smarter-missiles/>.

[49] MBDA Missile Systems, "MBDA Unveils Its Vision to Future Air Systems," June 17, 2019, available at <https://www.mbda-systems.com/press-releases/mbda-unveils-its-vision-of-future-air-systems/>.

[50] Scott Wierzbanowski, "Collaborative Operations in Denied Environment (CODE) (Archived)," Defense Advanced Research Projects Agency, available at. <https://www.darpa.mil/program/collaborative-operations-in-denied-environment>.

[51] Shishir Gupta, "India Rethinks Buying U.S. Armed Drones," *Hindustan Times*, July 28, 2019, available at <https://www.hindustantimes.com/india-news/india-rethinks-buying-us-drones/story-lrXANhzediWzKLd6j9bsqJ.html>.

[52] Robert O. Work, "AI and Future Warfare," Mad Scientist Disruption and the Future Operational Environment Conference, Army Futures Command, April 24, 2019, available at <https://www.youtube.com/watch?v=CDQPbeWTK5w>.

[53] Defense Advanced Research Projects Agency, "OFFensive Swarm-Enabled Tactics (OFFSET)," available at <https://www.darpa.mil/work-with-us/offensive-swarm-enabled-tactics>.

[54] Pratyaksha Mitra, "Russia Develops 'Jihadi Aviation' Drones," *Newscast Pratyaksha*, July 11, 2019, available at <http://www.newscast-pratyaksha.com/english/russia-develops-jihadi-aviation-drones/>.

[55] Thomas Luna, "China Launched 119 Fixed-Wing Drones and Sets New World Record," *WeTalkUAV*, June 17, 2017, available at <https://www.wetalkuav.com/119-fixed-wing-drones-china/>.

[56] Ziyan UAV, " ZIYAN UAV-Swarming Attack," Youtube, May 8, 2019, available at <https://www.youtube.com/watch?v=IbGiuMPLo3M>; Nikolai Novichkov, "Airshow China 2018: Norinco Presents UAV Swarm Concept," *Jane's Defence Weekly*, November 9, 2018, available at <www.janes.com/article/84438/airshow-china-2018-norinco-presents-uav-swarm-concept>.

[57] DARPA, "OFFensive Swarm-Enabled Tactics (OFFSET)."

[58] Jack Collier, "Unmanned Systems Technologies in Contested Urban Environments," *Unmanned Systems Technology* XXI, vol. 11021, available at <http://spie.org/Publications/Proceedings/Paper/10.1117/12.2519123>.

[59] Chong Shen et al., "Brain-like Navigation Scheme Based on MEMS-INS and Place Recognition," *Applied Sciences* 9, no. 8 (2019): 1708, available at <https://www.researchgate.net/publication/332664344_Brain-ike_Navigation_Scheme_based_on_MEMS-INS_and_Place_Recognition>; Xiao-chun Liu et al., "Image Mosaicing Using Inertial Navigation System for Increasing Match Information in Scene Matching Navigation System," *DEStech Transactions on Computer Science and Engineering* (2019), available at <http://www.dpi-proceedings.com/index.php/dtcse/article/view/28742>.

[60] Jen Dudson, "Soon to Come to the Army: A High-Power Microwave to Take Out Drone Swarms," *Defense News*, August 7, 2019, available at <https://www.defensenews.com/digital-show-dailies/smd/2019/08/07/the-armys-indirect-fires-protection-system-is-getting-a-high- power-microwave/>;Task and Purpose, "Check Out the Air Force's Futuristic 'Thor' Anti-Drone Microwave Gun," *The National Interest*, July 26, 2019, available at <https://nationalinterest.org/blog/buzz/check-out-air-forces-futuristic-thor-anti-drone-microwave-gun-69292>.

[61] Mathew Griffin, "Pentagon Tests Artificial Intelligence Electronic Warfare System," *311 Institute*, September 8, 2016, available at <https://www.311institute.com/pentagon-tests-artificial-intelligence-electronic-warfare-systems/>.

[62] Omer Herekoglu et al., "Flight Testing of a Multiple UAV RF Emission and Vision Based Target Localization Method," AIAA Scitech 2019 Forum, available at <https://arc.aiaa.org/doi/abs/10.2514/6.2019-1570>.

[63] David Luong and Bhashyam Balaji, "Quantum Radar, Quantum Networks, Not-So Quantum Hackers," *Signal Processing, Sensor/Information Fusion and Target Recognition XXVIII* (2019), available at <http://spie.org/Publications/Proceedings/Paper/10.1117/12.2519453>; David Luong and Bhashyam Balaji, "Radar Applications of Quantum Squeezing," *Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII* (2019), available at <http://spie.org/Publications/Proceedings/Paper/10.1117/12.2518530>.

[64] Victor Tangermann, "Electronic Warfare 'Disables' U.S. Aircraft in Syria," *Futurism*, April 26, 2018, available at <https://futurism.com/electronic-warfare-disables-aircraft-syria>; Task and Purpose, "The U.S. Military Is Getting Very Serious about Electronic Warfare," *The National Interest*, June 4, 2019, available at <https://nationalinterest.org/blog/buzz/us-military-getting-very-serious-about-electronic-warfare-61052>.

[65] Ibid.

[66] Ibid.

[67] Kyle Mizokami, "China Claims It Developed 'Quantum' Radar To See Stealth Planes," *Popular Mechanics*, September 22, 2016, available at <https://www.popularmechanics.com/military/research/a22996/china-quantum-stealth-radar/>.

[68] Chinese Academy of Sciences, "Beijing-Shanghai Quantum Communication Network put into Use," September 1, 2017, available at <http://english.cas.cn/newsroom/news/201703/t20170324_175288.shtml>.

[69] TRADOC Pamphlet 523-3-6, "The U.S. Army Functional Concept for Movement and Maneuver."

[70] Anna Varfolomeeva, "Signaling Strength: Russia's Real Syria Success Is Electronic Warfare Against the U.S.," *The Defense Post*, May 1, 2018, available at <https://thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/>.

[71] "Featured Research, Dr. Niranjan Suri, System complexity demands agility," *Florida Institute for Human and Machine Cognition* 10, no. 2 (2013), available at <https://www.ihmc.us/wp-content/uploads/2015/08/IHMCNewslettervol10iss2.pdf>.

[72] T. X. Hammes, "The Melians' Revenge: How Small, Frontline, European States Can Employ Emerging Technology to Defend Against Russia," *The Atlantic Council*, June 27, 2019, available at <https://www.atlanticcouncil.org/publications/issue-briefs/the-melians-revenge-how-small-frontline-european-states-can-employ-emerging-technology-to-defend-against-russia>.

[73] Mark Pomerleau, "To Win Future Conflicts, Combatant Commands Must Be Integrated." *C4ISRNET*, August 14, 2018, available at <https://www.c4isrnet.com/show-reporter/dodiis/2018/08/14/to-win-future-conflicts-combatant-commands-must-be-integrated/>.

[74] Elsa Kania, "All Titans Entangled," Hoover Institute, October 29, 2018, available at <https://www.hoover.org/research/ai-titans-entangled>.

[75] Tabriz Aniseh Bassiri and Justin Bronk, "Armed Drones in the Middle East: Proliferation and Norms in the Region," Royal United Services Institute, Occasional Papers, December 17, 2018, available at <https://www.rusi.org/publication/occasional-papers/armed-drones-middle-east-proliferation-and-norms-region>.

[76] Feng Xuejun and Li Qiang, "China's BeiDou Navigation System to Cover Globe by 2020," *People's Daily*, June 21, 2019, available at < https://www.telegraph.co.uk/peoples-daily-online/science/beidou-gps-satellite-navigation-complete/>.

[77] Eric H. Arnett, "Welcome to Hyperwar," *Bulletin of the Atomic Scientists* 48, no. 7 (September 1992): 14–21, available at <https://www.tandfonline.com/doi/pdf/10.1080/00963402.1992.11460097>.

[78] International Institute of Strategic Studies, "China's Pursuit of Advanced Dual-Use Technologies," December 18, 2018, available at <https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance>.

[79] Zachary S. Davis, "Artificial Intelligence in the Battlefield." *Livemore Research Laboratory*, Center for Global Security Research, March 2019, available at <https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf>.

[80] Ibid.

[81] Marcelo Kano-Kollmann et al., "Burying the Hatchet for Catch-up: Open Innovation Among Industry Laggards in the Automotive Industry," *California Management Review* 60, no. 2 (2018): 17–42, available at <http://eprints.exchange.isb.edu/554/>.

[82] DefAero Report, "NATO's Sharpy on Alliance Capability Development, Exercises, Wargaming," December 2018, available at <https://defaeroreport.com/2018/12/18/cancel-save-changes-natos-sharpy-on-alliance-capability-development-exercises-wargaming/>.

[83] Aaron Mehta, "U.S., India Collaborating on Air-launched Drone," *South Asian Monitor*, March 20, 2019, available at <https://southasianmonitor.com/2019/03/20/us-india-collaborating-on-air-launched-drone/>.

[84] Office of the Under Secretary of Defense for Acquisition and Sustainment, "U.S.-India Defense Technology and Trade Initiative (DTTI)," available at <https://www.acq.osd.mil/ic/DTTI.html>.

[85] Crunchbase, "Softbank," available at <https://www.crunchbase.com/organization/softbank#section-funds-raised>.

[86] Robert O. Work and Greg Grant, "Beating the Americans at Their Own Game, An Offset Strategy with Chinese Characteristics," Center for New American Security, June 6, 2019, available at <https://www.cnas.org/publications/reports/beating-the-americans-at-their-own-game>.

[87] Douglas Frantz, "We've Unleashed AI. Now We Need a Treaty to Control It," *Los Angeles Times*, July 16, 2018, available at <https://www.latimes.com/opinion/op-ed/la-oe-frantz-artificial-intelligence-treaty-20180716-story.html>.

National Defense University
Alumni Continuing Education
Security Seminar (ACESS)
September 14-19, 2020
Sydney, Australia

For information contact Devin Hess and Blake Traeger (ismo@ndualumni.org)

An aircrew from the California Air National Guard's 163rd Attack Wing flies an MQ-9 Reaper remotely piloted aircraft during a mission to support state agencies fighting the Mendocino Complex Fire in Northern California, Aug. 4, 2018. (Senior Airman Crystal Housman)

The Ethics of Acquiring Disruptive Technologies

Artificial Intelligence, Autonomous Weapons, and Decision Support Systems

By C. Anthony Pfaff

Last spring, Google announced that it would not partner with the Department of Defense (DOD) on "Project Maven," which sought to harness the power of artificial intelligence (AI) to improve intelligence collection and targeting, because its employees did not want to be "evil."[1] Later that fall, the European Union called for a complete ban on autonomous weapons systems.[2] In fact, a number of AI-related organizations and researchers have signed a "Lethal Autonomous Weapons Pledge" that expressly prohibits development of machines that can decide to take a human life.[3]

Reluctance to develop AI applications for military purposes is not going to go away as the development, acquisition, and employment of these systems challenge the traditional norms associated with not just warfighting but morality in general.[4] Meanwhile, as the debate rages, adversaries of the United States who do not have these ethical concerns continue with their development. China, for example, has vowed to be the leader in AI by 2030.[5] No one should have any illusions that the Chinese will not use this dominance for military as well as civilian purposes. So, to maintain parity, if not advantage, DOD has little choice but to proceed with the development and employment of artificially intelligent systems. As it does so, ethical concerns will continue to arise, potentially excluding important expertise for their development. To include this expertise, DOD needs to confront these concerns upfront.

Because this technology challenges traditional norms, it is disruptive in ways that more conventional technologies are not. This disruption arises because these technologies do not simply replace older ones but change how actors compete.[6] Changing how actors compete in effect changes the game—which, in turn, changes the rules. To effectively compete in the new environment, actors then have to establish new rules. For example, the development of the internet changed how people obtained news and information, forcing the closure of more traditional media, which struggled to find ways to generate revenue under these new conditions.

Of course, in addressing ethical concerns, it is important to be clear regarding the source of the "evil" in question. To the extent opponents of the technology are committed pacifists, then there is little reason one could bring to bear to change their minds. Another way, however, of understanding their objection is not that all military research is evil, but that development and use of AI weapons systems are *mala en se*, which means

Dr. C. Anthony Pfaff is a Research Professor for Strategy, the Military Profession, and Ethics, Strategic Studies Institute, U.S. Army War College.

their use, in any context, constitutes a moral wrong. If true, such weapons would fall into the same category as chemical and biological weapons, the use of which is banned by international law. If these weapons do fit into that category, the U.S. Government's only morally appropriate response would be to work to establish an international ban rather than to develop them.

The difficulty here is that no one really knows if these weapons are inherently evil. Objections to their use tend to cluster around the themes that such weapons introduce a "responsibility gap" that could undermine international humanitarian law (IHL) and dehumanize warfare in ways that are morally unacceptable. Moreover, even if one resolved these concerns, the application of such systems risks moral hazards associated with lowering the threshold to war, desensitizing soldiers to violence, and incentivizing a misguided trust in the machine that abdicates human responsibility. At the same time, however, proponents of such systems correctly point out that they are not only typically more precise than their human counterparts, they also do not suffer from emotions such as anger, revenge, and frustration that give rise to war crimes.

The answer, of course, will depend on how DOD proceeds with the development of these systems. While the responsibility gap and dehumanization of warfare are important moral objections, there are ways to address them as well as the moral hazards to which these systems give rise. Addressing these objections, however, will require attention throughout the development, acquisition, and employment cycles.

For the purposes of this discussion, the term *AI systems* will refer to military AI systems that may be involved in life-and-death decisions. These systems include both lethal autonomous weapons systems (LAWS) that can select and engage targets without human intervention, and decision support systems (DSS) that facilitate complex decisionmaking processes, such as operational and logistics planning. After a brief discussion of military applications of AI, I will take on the question of whether these systems are *mala en se* and argue that the objections described above are insufficient to establish that they are inherently evil. Still, this is new and disruptive technology that gives rise to moral hazards that are unique to its employment. I will address that concern and discuss measures DOD can take to mitigate these hazards so that the employment of these systems conforms to our moral commitments.

The Responsibility Gap

Advocates of AI systems often make the point that these systems' capabilities enable ethical behavior better than that of human beings, especially in combat. Ronald G. Arkin, in his book *Governing Lethal Behavior in Autonomous Robots*, argues that not only do such systems often have greater situational awareness, they also are not motivated by self-preservation, fear, anger, revenge, or misplaced loyalty, suggesting that they will be less likely to violate the war convention than their human counterparts.[7] Improving ethical outcomes, however, is only part of the problem. While machines may perform ethically better than humans—in certain conditions at least—they still make mistakes.

The fact that machines can make mistakes entails the possibility for harm to persons for which no one is accountable. This point, however, is not intuitively obvious. Conventional weapons can also malfunction and result in unjust death or harm. That fact, however, does not generate concern regarding the rules for their employment or raise ethical concerns regarding their acquisition. As operators can trust these systems to generally function reliably and their effects conform to IHL, then usually there are no ethical reasons—beyond a general commitment to pacifism—to oppose their employment. When the employment of such systems does result in excessive or unjustified harm,

it is possible conceptually, if not always practically, to determine where the responsibility lies: with the operator, who may have used the system improperly; the manufacturer, which may have made an error in the systems construction; or the developer, who may have designed the system poorly. The source, whatever it is, is human, and humans can be held accountable for their actions.

AI-driven systems, however, erode that trust in two ways. First, rather than simply being instrumental to human decisions, they take some of the burden of that decisionmaking off of humans. Moreover, as the technology becomes more effective, humans will likely become more dependent on these machines for making life-and-death decisions. In Iraq, for example, some units employed a DSS to select the safest route for convoys to travel. It made this recommendation based on attack and other incident data it received.

In one instance, the machine recommended a route on which a convoy suffered an attack where U.S. soldiers' lives were lost. As it turned out, the recommended route had previously been categorized as one of the most dangerous routes in the area of operations. Because it was one of the more dangerous routes, convoys stopped using it; thus, over time, it appeared from the perspective of the DSS as one of the safer routes since there had not been any recent recorded attacks.[8] This is, of course, a simple example from a very rudimentary DSS. However, it does raise the question: on what basis can an operator reasonably trust an AI-driven system?

Second, as these machines become more complex, it may not always be possible to tell why they behaved the way they did. For example, in June 2007, the first three "Talon" Special Weapons Observation Reconnaissance Detection Systems—remotely controlled robots that can aim at targets automatically—were deployed to Iraq but reportedly never used because their guns moved when they should not have.[9]

To mitigate the hazards of unaccountable moral failure, one has to ensure that either a human makes life-and-death decisions or that machines develop the capability to act as "autonomous moral agents." Both give rise to moral concerns unique to AI systems. Keeping a human in the decisionmaking process often means that one cannot take full advantage of the capabilities of LAWS and DSS.[10] When that decision is to fire at a rapidly approaching missile, any delay can make the difference between life and death. Additionally, employing such systems risks desensitizing soldiers, lowering the threshold for violence, and developing a bias favoring machine judgments over human ones, which I will take up later.

To understand the difficulty in resolving these concerns, it will help to understand what it would take to turn AI systems into what Wendell Wallach and Colin Allen call "autonomous moral agents." They argue in their book, *Moral Machines: Teaching Robots Right from Wrong*, that moral agents require the ability to "monitor and regulate their behavior in light of the harms their actions may cause or the duties they may neglect."[11] Moreover, they further require the ability to "detect the possibility of harm or neglect of duty" as well as to take steps to minimize or avoid any undesirable outcomes.[12] There are two routes to achieving this level of agency. First is for designers and programmers to anticipate all possible courses of action and determine rules that result in desired outcomes in the situations in which the autonomous system will be employed. Second is to build "learning" systems that can gather information, attempt to predict consequences of their actions based on that information, and determine an appropriate response.[13] The former requires either a great deal of knowledge on the part of the programmer or a very limited application for the machine. The latter requires overcoming the related problems of ascription and isotropy.

Ascription refers to the way humans infer other persons' intent from their actions. *Isotropy* refers to

the human ability to determine the environmental elements or background knowledge relevant to that ascription. Consider, for example, a group of soldiers who burst into a room looking for an insurgent and see several young children with knives running in their direction. On what basis do they consider the children a threat? If the operation were conducted in a Sikh village, these soldiers might know that Sikhs often wear a traditional dagger, which is symbolic and never used as a weapon. Moreover, they might be able to discern from the way the children were running and other relevant environmental cues that the children were at play and not to be taken as a threat.[14]

To program that capability in a robot would also be a daunting, perhaps impossible, challenge. Ascribing mental states to others requires humans to see in others the beliefs, desires, hopes, fears, intentions, and so on, that they see in themselves. As Marcello Guarini and Paul Bello observe, the relevant information associated with such ascriptions is extensive and includes such diverse things as "facial expressions, gaze orientation, body language, attire, information about the agent's movement through an environment, information about the agent's sensory apparatus, information about the agent's background beliefs, desires, hopes, fears, and other mental states."[15]

This difficulty is frequently referred to as the frame problem. Human knowledge about the world is holistic, where changes in one bit of knowledge can affect others. For example, learning that one is out of milk may require one to schedule a grocery shopping trip, which in turn might cause one to reschedule a meeting as well as determine to buy more milk than one had previously done. While humans do this easily, a computational AI system must go through all of its stored information to test how running out of milk affects it.[16]

Even when an AI system can reasonably handle sorting through alternatives, its output—whether it is behavior or a course of action—lacks intention, an important component to moral analysis. In his famous "Chinese room" thought experiment, philosopher John Searle described a man who sits in a room. His job is to take input, in the form of Chinese characters, and consult a rule book that tells him what the output should be. He then takes the appropriate characters and provides them to whomever is outside the room. He does not understand the meaning of the characters, only how they relate to the rules. Thus, given a sufficiently complex rule book, he conceptually can mimic a fluent Chinese speaker without understanding anything being said.[17] Moreover, while he may be causally responsible for the output, since he does not understand it, he cannot be said to intend its content. If he does not intend the content of the response, it can further be concluded that he is indifferent to it.

The point here is that one thing at least that differentiates humans from machines is that humans, in the words of AI theorist John Haugeland, "give a damn." He argues that understanding language depends on caring about not only one's self, but also the world in which one lives.[18] The human in the Chinese room may care (or at least has the ability to care) that he gets the rules right, but the machine itself does not have the capacity to care what the output actually means. There is a difference between something being manipulated according to a set of rules and someone acting on one's volition according to rules.[19] The output of the Chinese room is clearly an example of the former.

This point suggests that AI systems will be limited in how they can interpret a complex environment, inviting error in their decisionmaking even when all the humans involved in their employment have done everything right. As Wallach and Allen also observe, "As either the environment becomes more complex or the internal processing of the computational system requires the management of a wide array of variables, the designers and

engineers who built the system may no longer be able to predict the many circumstances the system will encounter or the manner in which it will process new information."[20] If it is not possible to fully account for machine behavior in terms of decisions by human beings, then it is possible to have an ethical violation for which no one is responsible.

Further complicating accountability is the fact that not all AI-driven behavior is attributable to written code. As Paul Scharre and Michael Horowitz observe, at least some of the information certain AI systems use to determine their responses is often encoded in the strength of connections of their neural networks and not as code that human operators can analyze. As a result, machine thinking can be something of a "black box."[21] Thus, the inability to fully account for machine behavior introduces a "responsibility gap," which threatens to undermine the application of the war convention.[22] This gap is not just a function of accessibility and complexity. It also follows from the fact these machines can make mistakes or commit an unjustified harm even when they are functioning properly. Thus, the developer, manufacturer, and operator can do all the right things and unjustified harm can still be done.

To the extent AI systems cannot be morally responsible for the harm they cause, Hin-Yan Liu views the application of these systems as the moral equivalent of employing child soldiers who are also not morally responsible for the harm they commit. Rather, he argues, since international law criminalizes the introduction of children on the battlefield, regardless of how they behave, the crime for those who employ them is not simply that they are victimizing children, but that they are also introducing "irresponsible entities" on the battlefield. Since AI systems are also "irresponsible" in the relevant sense, they too should be banned and those who do introduce them subject to criminal penalty.[23]

The concern here is that accountability is a critical aspect of any normative regime. Norms, whatever form they come in, moral, legal, or practical, are the means by which we communicate to others that we hold them, and ourselves, accountable. However, when norms are not upheld, they die.[24] Consider a workplace environment where there is a norm, for example, to show up on time. If workers instead habitually show up late and are not held accountable, then they will likely continue to do so and others are likely to follow. Eventually, the norm to show up on time will cease to be a norm.

The employment of non-accountable AI systems risks the same fate to IHL as well as any other regulatory scheme governing the military. The fact that LAWS and DSS can absolve humans of accountability for at least some violations will establish an incentive to employ the machines more often and find ways to blame them when something goes wrong, even when a human is actually responsible. It is not hard to imagine that over time, there would be sufficient unaccountable violations that the rules themselves would rarely be applied, even to humans. This point suggests that it will be insufficient to defend the use of AI systems simply because they can be necessary, proportionate, discriminate, and avoid unnecessary suffering if their use threatens to undermine the rules themselves.[25]

While Liu is right that the utilization of autonomous systems does introduce entities that cannot be held accountable for harms they commit, it is worth considering the significance of the objection. One response could be to note that while with conventional weapons humans are typically responsible for any harms, it is not the case that they are always *held* responsible. That being the case, it is not clear there is a moral difference between failing to hold someone responsible and there not being someone to hold responsible. It would seem both conditions are equally destructive to a normative framework.

The difference, of course, lies in the options one has to remedy the situation. The appropriate response to failing to hold wrongdoers accountable

is, obviously, to overcome whatever barriers there are to accountability. However, in cases where there is no one to be held accountable, the way forward is not so clear.

Whatever that way forward is, the first step would seem to lie in finding a way to establish "meaningful human control" over these systems. Unfortunately, there is no set standard for meaningful human control that could apply. At one extreme, activist groups such as the International Committee for Robot Arms Control argue that meaningful human control must entail human operators having full contextual and situational awareness of the target area. They also need sufficient time for deliberation on the nature of the target, the necessity and appropriateness of attack, and the likely collateral harms and effects. Finally, they must have the means to abort the attack if necessary to meet the other conditions.[26]

The difficulty with these criteria is that they hold the systems to a higher standard than nonautonomous weapons systems already in use. Soldiers and their commanders rarely have "full contextual and situational awareness of a target area." Even when they do, soldiers who fire their rifles at an enemy have no ability to prevent the bullet from striking wherever they aimed it. It seems odd, then, to ban future weapons based on higher standards than the ones that current weapons meet.[27] It makes less sense when one realizes that some of the capabilities that come along with autonomous weapons can set conditions for better moral decisionmaking.

So whatever standard for meaningful human control one employs, it should reflect the abilities as well as limitations humans actually have. To the extent the problem lies in the machine's ability to displace or undermine human agency, the remedy lies in restoring it. For AI-driven systems, this remedy entails diffusing responsibility throughout the development, production, and employment processes. To do so, DOD should ensure the following:

- acquisition officials, designers, programmers, and manufacturers, as well as commanders and operators, must fulfill their roles with the war convention in mind;
- commanders and operators must be knowledgeable not only regarding what the machine is doing, they also must be sufficiently knowledgeable regarding how the machine works so they better understand how it will interpret and act on instructions as well as provide output;
- commanders and operators must be in a position to prevent machine violations, either by ensuring they authorize all potentially harmful actions by the machine or by being able to monitor the operations of the machine and prevent them from happening; and
- systems in which operator intervention is not possible should only be employed in situations where commanders and operators can trust them to perform at least as well as human soldiers.

Such measures may represent the best humans can do to limit mistakes, but they will not *eliminate* them. Given that the possibility for unaccountable error endures, should we then declare AI-driven systems *mala en se*? The short answer is no. As Geoffrey S. Corn argues, while humanitarian constraints on the conduct of war are a "noble goal," they do not exhaust the war convention, which permits states to defend themselves and others from aggression. As Corn notes;

> *When these constraints are perceived as prohibiting operationally or tactically logical methods or means of warfare, it creates risk that the profession of arms—the very constituents who must embrace the law—will see it as a fiction at best or, at worst, that will feign commitment to the law while pursuing sub rosa agendas to sidestep obligations.*[28]

The concern here is not that soldiers will sidestep legal or moral obligations because upholding them represents excessive risk. There are, however, deeper obligations at play. States have an obligation not only to defend their citizens but also to ensure that those citizens who come to that defense have every advantage to do so successfully at the least risk possible.[29] Thus, any ban on LAWS or DSS, to the extent it limits chances for success or puts soldiers at greater risk, represents its own kind of moral failure.

While this point suggests it is premature to declare AI-driven systems inherently evil, it is also insufficient to fully establish their permissibility. It is not enough to point out that AI systems can lead to better ethical outcomes without fully accounting for the unethical ones. It may be permissible to accept some ethical "risk" regarding human incentives as these can be compensated for by additional rules and oversight. When those are inadequate, as I will discuss later, there are still other ways to address the responsibility gap given any particular human-machine relationship. This point suggests that where humans can establish sufficient control over these systems to be responsible for their behavior, their use would be permissible. The difficulty with this approach, however, is that such control usually comes at the expense of using this technology to its full capability. Moreover, such control over the machines ignores the impact on humans.

Dehumanizing Warfare

On the surface, concerns about dehumanizing warfare seem odd. War may be a human activity, but rarely does it feel to those involved like a particularly humane activity, often bringing out the worst in humans rather than the best. Thus, if LAWS and DSS can reduce some of the cruelty and pain war inevitably brings, it is reasonable to question whether dehumanizing war is really a bad thing. As Paul Scharre notes, the complaint that respecting human dignity requires that only humans make decisions about killing "is an unusual, almost bizarre critique of autonomous weapons . . . there is no legal, ethical, or historical tradition of combatants affording their enemies the right to die a dignified death in war."[30]

Scharre's response, however, misses the point. He is correct that AI systems do not represent a fundamentally different way for enemy soldiers and civilians to die than those that human soldiers are permitted to employ. The concern here, however, is not that death by robot represents a more horrible outcome than when a human pulls the trigger. Rather, it has to do with the nature of morality itself and the central role that respect for persons, understood in the Kantian sense as something moral agents owe each other, plays in forming our moral judgments.

Drawing on Kant, Robert Sparrow argues that respect for persons entails that even in war, one must acknowledge the personhood of those one interacts with, including the enemy. Acknowledging that personhood requires that whatever one does to another, it is done intentionally, with the knowledge that whatever the act is, it is affecting another person.[31] This relationship does not require communication or even the awareness by one actor that he or she may be acted upon by another. It just requires that the reasons actors give for any act that affects another human being take into account the respect owed that particular human being. To make life-and-death decisions absent that relationship subjects human beings to an impersonal and predetermined process, and subjecting human beings to such a process is *disrespectful* of their status as human beings.

Thus, a concern arises when *non-moral* agents impose *moral* consequences on moral agents. Consider, for example, an artificially intelligent system that provides legal judgments on human violators. It is certainly conceivable that engineers could design a machine that could take into account a larger quantity and variety of data than could a human judge. The difficulty with the judgment the machine

renders, however, is that the machine cannot put itself in the position of the person it is judging and ask, "If I were in that person's circumstances, would I have done the same thing?" It is the inability to not only empathize but then employ that empathy to generate additional reasons to act (or not act) that makes the machine's judgment impersonal and predetermined.[32]

Absent an interpersonal relationship between judge and defendant, defendants have little ability to appeal to the range of sensibilities human judges may have to get beyond the letter of the law and decide in their favor. In fact, the European Union has enshrined the right of persons not to be subject to decisions based solely on automated data processing. In the United States, a number of states limit the applicability to computer-generated decisions and typically ensure an appeals process where a human makes any final decisions.[33]

This ability to interact with other moral agents is thus central to treating others morally. Being in an interpersonal relationship allows all sides to give and take reasons regarding how they are to be treated by the other and to take up relevant factors that they may not have considered beforehand.[34] In fact, what might distinguish machine-made legal judgments from human ones is the human ability to establish what is relevant as part of the judicial process rather than in advance. That ability is, in fact, what creates space for sentiments such as mercy and compassion to arise. This point is why only persons—so far, at least—can show respect for other persons.

So, if it seems wrong to subject persons to legal penalties based on machine judgment, it seems even more wrong to subject them to life-and-death decisions based on machine judgment. A machine might be able to enforce the law, but it is less clear if it can

A Stryker vehicle commander interacts in real time with a Soldier avatar that is participating remotely from a collective trainer. The U.S. Army Research Laboratory, University of Southern California Institute for Creative Technologies, Combined Arms Center-Training and Program Executive Office for Simulation, Training and Instrumentation are developing the Synthetic Training Environment, which will link augmented reality with live training. (U.S. Army photo by Lt. Col. Damon "DJ" Durall)

provide justice. Sparrow further observes that what distinguishes murder from justified killing cannot be expressed by a "set of rules that distinguish murder from other forms of killing, but only by its place within a wider network of moral and emotional responses."[35] Rather, combatants must "acknowledge the morally relevant features" that render another person a legitimate target for killing. In doing so, they must also grant the possibility that the other person may have the right not to be attacked by virtue of their noncombatant status or other morally relevant feature.[36]

The concern here is not whether using robots obscures moral responsibility; rather, it is that the employment of AI systems obscures the good that humans *can* do, even in war. Because humans can experience mercy and compassion, they can choose not to kill, even when, all things being equal, it may be permissible.

The fact that AI-driven systems cannot have the kind of interpersonal relationships necessary for moral behavior accounts, in part, for much of the opposition to their use.[37] If it is wrong to treat persons as mere means, then it seems wrong to have a "mere means" be in a position to decide how to treat persons. One problem with this line of argument, which Sparrow recognizes, is that not all employment of autonomous systems breaks the relevant interpersonal relationship. To the extent humans still make the decision to kill or act on the output of a DSS, they maintain respect for the persons affected by those decisions.

However, even with semi-autonomous weapons, some decisionmaking is taken on by the machine—mediating, if not breaking, the interpersonal relationship. Here Scharre's point is relevant. Morality may demand an interpersonal relationship between killer and killed but as a matter of practice, few persons in those roles directly encounter the other. An Islamic State fighter would have no idea whether the bomb that struck him was the result of a human or a machine process; therefore, it does not seem to matter much which one it was. A problem remains, however, regarding harm to noncombatants. While, as a practical matter, they have no more experience of an interpersonal relationship than a combatant in most cases, it still seems wrong to subject decisions about *their* lives and deaths to a lethal AI system, just as it would seem wrong to subject decisions about one's liberty to a legal AI system. Moreover, as the legal analogy suggests, it seems wrong even if the machine judgment were the correct one.

This legal analogy, of course, has its limits. States do not have the same obligations to enemy civilians that they do toward their own. States may be obligated to ensure justice for their citizens but are not so obligated to citizens of other states. There is a difference, however, between promoting justice and avoiding injustice. States may not be obligated to ensure justice for citizens of another state; however, they must still avoid acting unjustly toward them, even in war. So, if states would not employ autonomous weapons on their own territory, then they should not employ them in enemy territory.[38]

Here, of course, conditions matter. States may not choose not to employ LAWS in their own territory in conditions of peace; however, given the stakes, they may reasonably choose to do so in war, precisely because they are less lethal. If that were to be the case, then the concern regarding the inherent injustice of AI-driven systems could be partially resolved. Of course, it is not enough that a state treats enemy civilians with the same standards it treats its own. States frequently use their own citizens as mere means to an end, so we would want a standard for that treatment that maintained a respect for persons.

For the action of a state to fully meet the standards necessary to count as respecting persons, it must be taken for the sake of all those who may be affected. This condition does not mean that some

may not be harmed; however, if all alternatives would result in the same harm to that person, then it makes sense to choose the alternative that harms the fewest persons. As Isaak Applbaum argues, "If a general principle sometimes is to a person's advantage and never is to that person's disadvantage, then actors who are guided by that principle can be understood to act for the sake of that person."[39] So, to the extent AI-driven systems do make targeting more precise than human-driven ones, as well as reducing the likelihood that persons will be killed out of revenge, rage, frustration, or just plain fatigue, then their employment would not put any persons at more risk than if those systems were not employed. To the extent that is the case, then arguably states are at least permitted, if not obligated, to use them. Because employing these systems under such conditions constitutes acting for the sake of those persons, it also counts as a demonstration of respect toward those persons, even if the interpersonal relationship Sparrow described is mediated, if not broken, by the machine.

Moral Hazards of AI Systems

While the use of AI systems may not be inherently evil, the dual concerns of responsibility and dehumanization suggest their use will give rise to a number of moral hazards that need to be addressed if states are to ethically use these systems to their full capability. Moral hazards arise when one person assumes greater risk because they know some other person will bear the burden of that risk.[40] Given the reduction in risk—both for political leaders who decide to use force as well as the combatants who employ it—the employment of AI systems will establish an incentive structure to ignore the moral risks described above. To address this concern, we need to have a better account of how moral autonomy relates to machine autonomy and how humans, who have moral autonomy, can relate to machines.

Psychological Effects: Desensitization and Trauma

In general, trends in military technology have been to distance soldiers from the killing they do. Crossbows allowed killing at greater distances than did swords, rifles farther than crossbows, cannons and artillery farther than rifles. What is different about autonomous weapons is that they do not just distance soldiers from killing, they can also distance soldiers from the decision to kill. While this is clearly true in fully autonomous systems, it can be true for semi-autonomous systems as well. As P.W. Singer notes in *Wired for War*;

> *By removing warriors completely from risk and fear, unmanned systems create the first complete break in the ancient connection that defines warriors and their soldierly values.*[41]

As Singer goes on to observe, the traditional warrior identity arises from conquering profound existential fear, "not the absence of it."[42] The result is a fighting force that is not merely distanced from risk, but disconnected from it altogether. As one Air Force lieutenant reportedly said about conducting unmanned airstrikes in Iraq, "It's like a video game. The ability to kill. It's like . . . freaking cool."[43]

Of course, desensitization is not the only reaction operators have had to the use of autonomous and semi-autonomous systems. In fact, in 2015 a large number of drone operators quit, some citing overwork and others citing the horrors they felt responsible for as reasons.[44] As Samuel Issacharoff and Richard Pildes observe, the use of LAWS has, in some cases at least, increased the individuation of responsibility for killing and thus brought about a greater sense of responsibility for the killing they do.[45]

One feature that increases sensitivity is the amount of time unmanned aerial vehicle (UAV) pilots spend observing their targets and then watching the effects and aftereffects of strikes they initiate. One U.S. operator, Brandon Bryant,

reported as a source of emotional stress the fact that after a strike, he would not only sometimes have to review the aftermath, but often watch his targets die. Recounting one strike in Afghanistan, he not only observed the strike but also the bodies and body parts afterward. One particularly disturbing image was watching one of the individuals struck. As he recalls, "It took him a long time to die. I just watched him. I watched him become the same colour [sic] as the ground he was lying on."[46]

This kind of interaction is typically not a feature of conventional strikes. As one UAV pilot put it, "I doubted whether B–17 and B–20 [sic] pilots and bombardiers of World War II agonized much over dropping bombs over Dresden or Berlin as much as I did taking out one measly perp in a car."[47] The point here is not that increased use of semi-autonomous and autonomous weapons will bring about more or less sensitivity to killing or trauma but rather that as the character of war changes, different persons will respond differently. The ethical imperative is that leaders pay attention to those changes and take steps to mitigate their ill effects.

Lowering the Threshold to War

Lowering risk to soldiers also lowers risk for civilian leadership when it comes to decisions regarding when to use such weapons. Of course, this concern is not unique to autonomous systems. Any technology that distances soldiers from the violence they do or decreases harm to civilians will lower the political risks associated with using that technology. The ethical concern here is to ensure that decreased risk does not result in an increase in the number of unjust uses of these weapons.[48] Otherwise, one offsets the moral advantage gained from greater precision.

As Christian Enemark argues, "Political leaders, having less cause to contemplate the prospect of deaths, injuries, and grieving families, might accordingly feel less anxious about using force to solve political problems."[49] Like concerns regarding desensitization, concerns regarding lowering the threshold to war may be overstated. While arguably the use of UAV strikes has expanded over the last decade, instances of escalation into wider conflict have not. Even in areas such as Pakistan, Yemen, and Somalia, where the United States is not at war, the conflict in question preceded the use of unmanned systems, not the other way around. Thus, the ethical question is whether, if this technology were not available, the United States would (and should) do *something*. If the answer is yes, then to the extent the use of force is just and the use of LAWS makes the use of force more precise and humane, it is at least permissible. If the answer is no, then it is likely that no force would be permissible.

The difficulty in resolving this concern is that, much like the concern regarding desensitization, it pits a psychological claim regarding human motivations to employ violence against moral claims associated with the permissibility of violence. The answer to one question is not an answer to the other. Thus, while it may be true that lower risks make decisions about using force easier, it is irrelevant to whether such force is permissible. Having said that, to the extent the psychological concern is valid, it makes sense to confirm that decisions to use risk-decreasing weapons are subject to strict oversight to ensure the conditions of justice are met as well as any other measures that might mitigate these effects. The absence of this oversight and transparency is, in fact, often cited in the literature as a genuine moral concern and has been a longstanding criticism of the U.S. UAV operations.[50] Given this concern, it makes sense to ensure such oversight and transparency are in place. In this way one can ensure the human reliance on the machine does not set humans up for moral failures they may otherwise not make.

Another concern is that even when LAWS are employed ethically in the service of legitimate U.S. interests, their use may drag the United States into local conflicts of questionable justice. Enemark

notes a debate within DOD regarding whether such strikes are permitted only against high-value targets or also against the larger number of low-level militants whose concerns are more local. He observes that the narrower set is more defensible as preemptive strikes to the extent these individuals are actively plotting against the United States whereas lower-level militants are motivated to fight for local concerns. As he states;

> *The narrow view is more easily defensible because individuals who are actively plotting to attack the United States more obviously attract (pre-emptive) defensive action than do individuals who merely happen to possess an antipathy towards the United States.*[51]

Of course, this concern arises as much out of the fact that networks of terrorists threatening the United States draw on and cooperate with networks of oppositionists whose concerns are local, sometimes to the point where it is difficult to distinguish between the two. Thus, regardless of the means used, engaging the former risks expanding conflict with the United States to the latter, who would not otherwise be a threat. While this concern is real, it is more a feature of the character of the conflicts the United States finds itself in rather than the weapons system itself. In fact, it is conceivable that AI-assisted analysis could increase the U.S. military's capability to differentiate between these local and transnational networks. Having said that, the fact of this dynamic suggests the United States should adopt the narrower policy and employ a principle of conservatism when pressure to expand targeting to local targets increases. It may be permissible to do so; however, there should be a demonstrable relationship between the putative target and any threat to the United States.

Automation Bias

One other concern, touched upon earlier, is that humans can sometimes depend too much on the machine for decisions. One of the most often cited examples of this phenomenon is the shootdown of Iranian Air flight 655 by USS *Vincennes* in 1988. The USS Vincennes was equipped with the Aegis ballistic missile defense system, which is fully autonomous but has humans monitoring it as it goes through its targeting cycle. Humans can override the system at any point in this cycle and, in fact, the system was set to its lowest degree of autonomy. The jet's path and radio signature were consistent with civilian airliners; however, the system registered the aircraft as an Iranian F–14 and thus as an enemy. Though the data was telling the crew the aircraft was civilian, they trusted the computer's judgment and shot it down anyway, resulting in the deaths of 290 passengers.[53]

The difficulty for humans in situations like this is that the complexity of machine "thinking" coupled with the pressure to act, especially in combat, disposes them to trust the machine, especially when doing so can absolve them of at least some of the responsibility of the action in question as well as avoid the consequences of inaction. Moreover, that trust can emerge independent of the reliability of the machine. One study conducted by Korean researchers indicated that the most important factors in human assimilation of DSS were institutional pressure, mature information technology infrastructure, and top management support. Quality of information, stated the report, had no significant impact on DSS assimilation.[54]

Thus, the concern with such systems is that even though humans can prevent wrongful machine behavior, often they will not. That counterintuitive outcome arises from the fact that what the machine often presents to the human is a judgment, but the human takes it as fact. This certainly seemed to be case in the shootdown of the Iranian airliner. The *fact* was that there was an aircraft approaching *Vincennes*, which the system judged was enemy. From the context, specifically the flight path and

radio signature, the humans on board should have questioned the machine and aborted the attack.[55] As machine judgments become more complex, this concern is only going to be heightened.

This point suggests that operators are going to need to develop sufficient expertise to know what sources of bad judgment are. It will also require operators to adopt a "principle of conservatism" regarding when they should trust the machine without corroborating its output, and limit those times to only what is necessary to accomplishing the mission at hand. To facilitate that trust, as Scharre and Horowitz argue, designers will have to do their best to ensure the outputs of AI systems are "explainable" to at least the operator, if not the commander.[56]

The good news here, as Scharre points out, is that the most successful AI systems will be those that rely on human-machine interaction, suggesting the most successful systems will have a human integrated into the decision cycle.[57] These systems, which he refers to as "Centaur systems," are intentionally designed to maximize the speed and accuracy of a hybrid human-machine system in given situations. Examples include defensive systems such as the counter-rocket, artillery, and mortar systems that autonomously create "do not engage" sectors around friendly aircraft. These systems have a human fail-safe to ensure engagements outside those sectors avoid fratricide or harm to civilian aircraft that might approach too closely.[58]

Conclusion

What this analysis has shown is that the arguments for considering military AI systems, even fully autonomous ones, *mala en se* are on shakier ground than those that permit their use. It is possible to reduce, if not close, the responsibility gap and demonstrate respect for persons even in cases where the machine is making all the decisions. This point suggests that it is possible to align effective AI systems development with our moral commitments and conform to the war convention.

Thus, calls to eliminate or strictly reduce the employment of such weapons are off base. If done right, the development and employment of such weapons can better deter war or, failing that, reduce the harms caused by war. If done wrong, however, these same weapons can encourage militaristic responses when other nonviolent alternatives were available, resulting in atrocities for which no one is accountable, and desensitizing soldiers to the killing they do. To promote the former and avoid the latter, the United States should consider the following measures to ensure the ethical employment of these weapons systems:

- *Work with AI-developing states to update international law.* As previously discussed, international law abhors a vacuum and makes the introduction of any system that mitigates or removes human responsibility problematic. On the other hand, many AI-developing states will take advantage of this vacuum to maximize the effectiveness of these systems, sometimes, if not often, without regard to the moral concerns discussed above. This point suggests the need to update the IHL and other applicable international law, to specify standards of responsibility for the employment of semi-autonomous and fully autonomous systems. These standards would include something like;
    - Operators would have to justify trust in any facts or judgments made by the machine. If that justification is inadequate, they may be responsible for any violations.
    - Operators should ensure AI systems are only employed in conditions for which they are designed to perform ethically. They are also responsible for monitoring the environment and the machine and ceasing operations when conditions changes in a way that sets conditions for violations.

- *Establish standards for diffusing responsibility.* States should establish standards for holding acquisition officials, programmers, designers, and manufacturers responsible for machine violations. These standards will be especially important for fully autonomous systems where conditions for trust by commanders and operators are heavily dependent on the procurement side for ensuring that the machine meets standards associated with operational and functional morality. Meeting such standards would entail accounting for IHL when determining the features of the machine in the same way one might incorporate a safety device on a rifle.
- *Maintain a reasonably high threshold for use.* To ensure employment of AI systems does not inappropriately lower the threshold to violence, states should agree to only employ these systems when the conditions of *jus ad vim* are met. These conditions permit an armed response for acts of aggression that fall short of war, but include the other standards of *jus ad bellum* as well as the requirement to take steps to avoid escalation. *Jus ad vim* also entails an obligation to ensure a high degree of probability that the use of force will achieve the desired objective.[59]
- *Specify conditions for employment.* Given the different human-machine relationships, states should specify conditions for use that ensure meaningful human control and the appropriate trust relationships are maintained. Update these standards as the technology evolves to avoid further gaps between effective use of AI systems and moral commitments.
- *Regulate AI proliferation.* States that develop AI systems for military use should establish proliferation standards similar to the ones the United States has established for the proliferation of UAVs. At a minimum, these standards should include a commitment to only employ these systems in conflicts that meet the standards of *jus ad bellum* and in a manner that meets the standards of *jus in bello*. Moreover, there should be a strong presumption of denial to recipients of the technology who have, in the past, been weak on their commitments to these standards.[60]
- *Preserve the soldier identity and address conditions that give rise to desensitization and other psychological trauma.* As the U.S. military becomes more reliant on AI technology, soldiers will experience less risk, but not less trauma. Senior leaders should continue efforts to understand the nature of this trauma and take steps to mitigate it. Moreover, disconnecting soldiers from the risk will also affect how society views and rewards military service. Senior leaders should take steps now to mitigate this potential moral hazard. One step could be to rotate AI system operators in and out of assignments that expose them to risks commensurate with the conflict in question. Doing so will prevent the creation of a class of "riskless" soldiers and moderate the impact of this technology on civil-military relations.
- *Communicate the principles regarding AI use.* Military leaders should develop a communications plan to explain the ethical framework for AI use to the public, media, and Congress.[61]

As Sharkey observes, the heavy manpower requirements with remotely controlled systems will place greater pressure to design and employ increasingly autonomous systems.[62] This point, coupled with the increased effectiveness these systems afford, suggests the trend toward fully autonomous systems is inevitable. As this pressure mounts, commitments to keep humans in the decision process will be increasingly difficult to uphold. Fortunately, as the above analysis indicates, it is possible to manage the moral hazards associated with this technology to ensure moral commitments to human dignity, the rule of law, and a stable international

order are met. Doing so may not assuage every Google employee; however, it will ensure that in acquiring these systems, the United States avoids evil. PRISM

Notes

[1] Scott Shane, Cade Metz, and Daisuke Wakabayushi, "How a Pentagon Contract Became an Identity Crisis for Google," *New York Times*, May 30, 2018, available at <https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html>. It is worth noting that Google's commitment to avoiding evil is less than consistent, given its proposed cooperation with the Chinese government to provide a censored search engine. See Rob Schmitz, "Google Plans for a Censored Search Engine in China," National Public Radio, August 2, 2018, available at <https://www.npr.org/2018/08/02/635047694/google-plans-for-a-censored-search-engine-in-china>.

[2] "Thursday Briefing: EU Calls for Ban on Autonomous Weapons," *Wired*, September 18, 2018, available at <https://www.wired.co.uk/article/wired-awake-130918>.

[3] Future of Life Institute, "Lethal Autonomous Weapons Pledge," available at <https://futureoflife.org/lethal-autonomous-weapons-pledge/?cn-reloaded=1>.

[4] For the purposes of this discussion, the term AI systems will refer to military *AI systems* that may be involved in "life-and-death" decisions. These systems include both lethal autonomous weapons systems that can select and engage targets without human intervention and decision support systems that facilitate complex decisionmaking processes, such as operational and logistics planning.

[5] Paul Mozur, "Beijing Wants AI to be Made in China by 2030," *New York Times*, July 20, 2017, available at <https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html>.

[6] Erwin Danneels, "Disruptive Technology Reconsidered: A Critique and Research Agenda," *Journal of Product Innovation Management* 21, no. 4 (July 2004), 21, 249.

[7] Ronald G. Arkin, *Governing Lethal Behavior in Autonomous Robots* (Boca Raton, FL: Chapman and Hall, 2009), 30.

[8] Colonel James Boggess, interview with author, January 4, 2017.

[9] Noel Sharkey, "Killing Made Easy," in *Robot Ethics*, ed. Patrick Lin, Keith Abney, and George A. Berkey (Cambridge, MA: MIT Press, 2014), 113.

[10] Much of the literature describes human interaction in terms of "humans in the loop," where the human makes decisions for the machine; "humans on the loop," where humans monitor the machine and only act to prevent it from acting error; and "humans off the loop," where humans provide no additional direction to the machine once it is set in operation. These terms, however, are somewhat imprecise, as in all the three instances, humans played a role in how the machine made a decision, whether in design, production, or employment. Because of this imprecision, I will avoid use of these terms for this discussion.

[11] Wendell Wallach and Colin Allen, *Moral Machines: Teaching Robots Right from Wrong* (New York: Oxford University Press, 2009), 16.

[12] Ibid.

[13] Ibid.

[14] Marcello Guarini and Paul Bello, "Robotic Warfare: Some Challenges in Moving from Noncivilian to Civilian Theaters," in Lin, Abney, and Berkey, *Robot Ethics*, 129–130.

[15] Ibid., 131–132.

[16] Zed Adams and Jacob Browning, "Introduction," in *Giving a Damn: Essays in Dialogue with John Haugeland*, ed. Zed Adams and Jacob Browning (Cambridge, MA: MIT Press, 2017), 4.

[17] Kevin Warwick, "Robots with Biological Brains," in Lin, Abney, and Bekey, *Robot Ethics*, 327–328.

[18] Adams and Browning, 5.

[19] Ibid., 13.

[20] Wendell Wallach and Colin Allen, "Framing Robot Arms Control," *Ethics of Information Technology* 15 (2013), 127.

[21] Paul Scharre and Michael Horowitz, *Artificial Intelligence: What Every Policy Maker Needs to Know* (Washington, DC: Center for a New American Security, June 2018), 11, available at <https://www.cnas.org/publications/reports/artificial-intelligence-what-every-policymaker-needs-to-know>. As an example of "black box" thinking, Scharre and Horowitz note that an "AI image recognition system may be able to identify the image of a school bus, but not be able to explain what features of the image cause it to conclude that the picture is a bus."

[22] Heather Roff, "Killing in War: Responsibility, Liability, and Lethal Autonomous Robots," in T*he Routledge Handbook of Ethics in War*, ed. Fritz Allhoff, Nicholas G. Evans, and Adam Henschke (New York: Routledge, 2013), 355.

[23] Hin Yan Liu, "Refining Responsibility: Differentiating Two Types of Responsibility Issues Raised by Autonomous Weapons Systems," in *Autonomous Weapon Systems: Law, Ethics, Policy*, ed. Nehal Bhuta et al. (Cambridge: Cambridge University Press, 2016), 341–344.

[24] Geoffrey Brennan et al., *Explaining Norms*

(Oxford: Oxford University Press, 2013), 35–39.

[25] These principles are also stated in Army doctrine. See Army Doctrine Reference Publication (ADRP) 1, *The Army Profession* (Washington, DC: Headquarters, Department of the Army, June 2015), 3–5. I owe this point to Michael Toler, Center for the Army Profession and Ethic.

[26] Noah Sharkey, "Guidelines for the Human Control of Weapon Systems," International Committee for Robot Arms Control, April 2018, available at <https://www.icrac.net/wp-content/uploads/2018/04/Sharkey_Guideline-for-the-human-control-of-weapons-systems_ICRAC-WP3_GGE-April-2018.pdf>.

[27] Scharre and Horowitz, *Autonomy in Weapons Systems*, 16.

[28] Geoffrey S. Corn, "Risk, Transparency, and Legal Compliance," in Bhuta et al., *Autonomous Weapon Systems*, 217–218.

[29] Michael Walzer, *Arguing About War* (New Haven: Yale University Press, 2004), 23–32.

[30] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton and Company, 2018), 287–288.

[31] Robert Sparrow: "Robots and Respect: Assessing the Case Against Autonomous Weapon Systems," *Ethics and International Affairs* 30, no. 1 (2016), 106. It is worth noting here that the Army Ethic acknowledges the importance of respect and includes as a principle, "In war and peace, we recognize the intrinsic dignity and worth of all people, treating them with respect." See ADRP 1, 2-7. I owe this point to Michael Toler, Center for the Army Profession and Ethic.

[32] Eliav Lieblich and Eyal Benvenisti, "The Obligation to Exercise Discretion in Warfare: Why Autonomous Weapons Systems Are Unlawful," in Bhuta et al., *Autonomous Weapon Systems*, 266.

[33] Ibid., 267.

[34] The point here is not that the battlefield is a place to negotiate or that there has to be some kind of interaction independent of a targeting process to justify the decision to use lethal force. Rather, the point is that in any given situation where a human being may be harmed that the decision made to commit that harm is made by another human who can identify and consider the range of factors that would justify that harm. In this way, the person deciding to harm understands it is another person whom he or she is harming and considers reasons not to do it. Autonomous systems may eventually be able to discern a number of relevant factors; however, that only entails they are considering reasons to harm, not reasons not to harm.

[35] Sparrow, "Robots and Respect," 101.

[36] Ibid., 106–107.

[37] Ibid., 108.

[38] Lieblich and Benvenisti, "The Obligation to Exercise Discretion in Warfare," 267.

[39] Arthur Isaak Applbaum, *Ethics for Adversaries: The Morality of Roles in Public and Professional Life* (Princeton, NJ: Princeton University Press, 1999), 162–166. Applbaum refers to situations where someone is better off and no one is worse off as "avoiding Pareto-inferior outcomes." Avoiding such outcomes can count as "fair" and warrant overriding consent.

[40] Kenneth J. Arrow: "Uncertainty and the Welfare Economics of Medical Care," *American Economic Review* 53, no. 5 (December 1963), 941, 961. See also Matthew McCaffrey, "Moral Hazard: Kenneth Arrow vs Frank Knight and the Austrians," MISES WIRE, March 14, 2017, available at <https://mises.org/blog/moral-hazard-kenneth-arrow-vs-frank-knight-and-austrians>.

[41] P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Books, 2009), 332.

[42] Ibid.

[43] Ibid., 395.

[44] Pratap Chatterjee, "American Drone Operators Are Quitting in Record Numbers," *The Nation*, March 5, 2015, available at <https://www.thenation.com/article/american-drone-operators-are-quitting-record-numbers/>.

[45] Samuel Issacharoff and Richard Pildes, "Drones and the Dilemmas of Modern Warfare," in *Drone Wars: Transforming Conflict, Law, and Policy*, ed. Peter Bergen and Daniel Rothenberg (Cambridge: Cambridge University Press, 2015), 399.

[46] Phillip Sherwell, "U.S. Drone Pilot Haunted by Horrors of Remote Killings; Operator Sickened by Death Count," *London Daily Telegraph*, October 25, 2013, available at <https://www.telegraph.co.uk/news/worldnews/northamerica/usa/10403313/Confessions-of-a-US-drone-operator-I-watched-him-die.-It-took-a-long-time.html>.

[47] Matt J. Martin and Charles Sasser, *Predator: The Remote-Control Air War over Iraq and Afghanistan: A Pilot's Story* (Minneapolis, MN: Zenith Press, 2010), quoted in Isaccharoff and Pildes, 416.

[48] Christian Enemark, *Armed Drones and the Ethics of War* (London: Routledge, 2014), 22.

[49] Ibid., 23.

[50] Sharkey, "Guidelines for the Human Control of Weapon Systems," 115. As Sharkey states, "It is now unclear what type and level of evidence is being used to sentence nonstate actors to death by Hellfire attack without right to appeal or right to surrender." The point here is not that U.S. targeting procedures are unjust, but to the extent they are not transparent—at least to the

extent possible without compromising the process—the perception of injustice will persist, generating the kind of response evidence by the Google employees.

[51] Enemark, *Armed Drones and the Ethics of War*, 25.

[52] I owe this point to Colonel David Barnes, Department of English and Philosophy, U.S. Military Academy at West Point.

[53] Singer, *Wired for War*, 125.

[54] Hyun-Ku Lee and Hangjung Zo, "Assimilation of Military Group Decision Support Systems in Korea: The Mediating Role of Structural Appropriation," *Information Development* 21, no. 1 (2017), quoted in James Boggess, "More than a Game: Third Offset and the Implications for Moral Injury," in *Closer than You Think: The Implications of the Third Offset Strategy* (Carlisle, PA: Strategic Studies Institute, 2017), 133.

[55] David Evans, "Vincennes: A Case Study," *Proceedings* 119, no. 8/1086 (August 1993).

[56] Scharre and Horowitz, *What Policy Makers Need to Know*, 11.

[57] Scharre, *Army of None*, 321.

[58] Ibid., 323–324.

[59] Daniel Brunstetter and Megan Braun, "From Jus ad Bellum to Jus ad Vim: Recalibrating our Understanding of the Moral Use of Force," *Ethics and International Affairs* 27, no. 1 (2013).

[60] Fact Sheet, "U.S. Policy on the Export of Unmanned Aerial Systems," U.S. State Department, April 19, 2018, available at <https://www.state.gov/r/pa/prs/ps/2018/04/280619.htm>. This policy is a little more permissive than the one implemented by the last administration. It permits the sale of armed unmanned systems through direct commercial sales and removes language regarding a "strong presumption of denial" for systems that cross the Missile Technology Control Regime thresholds, which in this case are systems with a range greater than 300 kilometers and are capable of carrying payloads of 500 kilograms or more. Both sets of standards require upholding international law. See Fact Sheet, "U.S. Policy on the Export of Unmanned Aerial Systems," U.S. State Department, February 17, 2015, available at <https://2009-2017.state.gov/r/pa/prs/ps/2015/02/237541.htm>.

[61] I owe this point to Dr. Steve Metz, Strategic Studies Institute, U.S. Army War College.

[62] Sharkey, "Guidelines for the Human Control of Weapon Systems," 115.

Extreme terrain discover technology

The Challenges Facing 21st Century Military Modernization

By Bernard F.W. Loo

When the Singapore Minister of Defense tabled the proposed budget for the Singapore Armed Forces for 2019–20 before the Parliament in February 2019, the Ministry of Defence issued an infographic that explained how the most recent military acquisitions—Type-219 submarines from Germany and the planned acquisition of F–35s from the United States being the most visible—would result in a next-generation Singapore Armed Forces that will be "more lethal in all domains."[1] At the other end of the spectrum of military power, the *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* emphasizes lethality as a fundamental, necessary characteristic of the United States military; indeed, the words "lethal" and "lethality" appear 16 times across its 11 pages of text.[2]

When a military organization undertakes a modernization program, it is intuitive to expect that existing capabilities are going to be replaced by superior capabilities. There is an implied suggestion that a necessary (though not sufficient) condition of this superiority is enhanced lethality; lethality surely constitutes a necessary condition of the strategic effectiveness of the military organization in question.[3] At the risk of stating the obvious, military organizations around the world exist to protect the security of their respective countries: in peacetime, by deterring the adversaries of the country from waging war, and in wartime, by defeating these adversaries should they choose the war option. These two missions are not mutually exclusive: "The surest way to prevent war is to be prepared to win one."[4] Nevertheless, it is possible to question the extent to which lethality subsequently connects to strategic effectiveness, which is understood here as the ability to win wars. In other words, while modernization ought to result in a military organization that is more lethal than before, this enhanced lethality does not guarantee strategic effectiveness.

Using the example of Singapore, this article will construct its argument by, first, proposing an ideal model of military modernization, based on questions that a country's policymakers and military planners ought to be asking themselves as they decide on how the country's military organization is to be modernized. Next, the article shifts its attention to the questions military planners and policymakers either ask (or ought to be asking) in deciding on specific modernization programs. Finally, the article examines the issue of strategic

Dr. Bernard F.W. Loo is a Senior Fellow with the Military Studies Programme, at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore.

effects, which is what military organizations ultimately seek to achieve. It is here that the question of the relationship between enhanced lethality and strategic effectiveness can be addressed.

Technological Development and Lethality

In *An Introduction to Strategic Studies: Military Technology and International Politics*, Barry Buzan argued that the phenomenon of the arms dynamic—and the process of military modernization is a manifestation of this concept—is driven by three elements: an action-reaction dynamic between the state and its putative adversary; the domestic structures within the state that are not necessarily fully synchronized with the action-reaction dynamic with its putative adversary; and a technological imperative within which the first two elements exist.[5] Interestingly, Buzan, together with Eric Herring, revisited this concept in the 1998 book, *The Arms Dynamic in World Politics*; now, the arms dynamic concept has been refined, where it is driven by two imperatives, namely action-reaction and domestic structures, and technology is the context in which the arms dynamic necessarily exists.

Why does this matter? This article attempts to construct an argument that is predicated on the assumption that technology plays an increasingly important role in shaping the modernization of military organizations. Furthermore, whether as imperative or as context, the technological landscape is increasingly complex, because a number of not necessarily military technologies can have strategic impact, including "computing, 'big data' analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology."[6]

Given that the ultimate function of any military organization is the protection of the state from external, and sometimes existential, threats, the desire for "better" weapons systems is intuitive and necessary; "better" is surely the path that military technological development takes, and this typically takes the form of enhanced lethality.[7] Modern technologies make existing weapons systems even more lethal. Indeed, in the aftermath of Operation *Desert Storm*, then-Chief of Staff of the U.S. Air Force, General Merrill A. McPeak, argued that the experience of *Desert Storm* demonstrated that the U.S. military needed to enhance its lethality by increasing investments in all-weather precision munitions that are cheap and therefore acquirable in large numbers.[8] Irrespective of the particular service, the *Summary of the 2018 National Defense Strategy of the United States of America* maintains this belief in lethality; the document paints a picture of a future battlefield that is;

> *ever more lethal and disruptive . . . combined over domains, and conducted at increasing speed and reach [by] competitors and adversaries [who] seek to optimize their targeting of our battle networks and operational concepts" by employing "other areas of competition short of open warfare to achieve their ends (e.g., information warfare, ambiguous or denied proxy operations, and subversion).*"[9]

Lethality is a function of a series of factors. The most immediately obvious factor is precision sensing and targeting, which allow you to "see" the enemy first and bring lethal fires to bear against it, with greater accuracy—an important consideration given the increasing costs of modern weapons systems—before the enemy can "see" your own forces.

In an age of computer networks and joint military operations, data linkages and bandwidths constitute a second, and enabling, factor; these are important considerations because they allow the military organization to do away with traditional interservice rivalries and function as a single, coherent entity, and to engage enemy forces (a euphemism for lethality) with any available weapons systems

deployed on air-, land-, or sea-based platforms.

The third factor is survivability. This is important, because if your weapons systems are more survivable than those of your adversary or enemy, it means your military organization can be more lethal than its counterpart.

The United States recognizes that its military organization has "no preordained right to victory" and therefore needs to be a "more lethal, resilient, and rapidly innovating Joint Force." This lethality is strategically vital for the military organization in its peacetime and wartime functions. A peacetime military organization seeks to dissuade—more precisely, deter—its adversary (or adversaries, as the case may be) from initiating hostile military operations against the state, whereas a wartime military organization seeks to defeat—more precisely, attain strategic success against—its enemy. This "more lethal force" can then "sustain American influence and ensure favorable balances of power that safeguard the free and open international order."[10] However, as I will discuss later, both deterrence and strategic success are problematic concepts, and neither concept is necessarily driven by lethality.

Military Modernization: Questions and Caveats

In any military modernization program, policymakers and military planners have to find a delicate balance in their answers to three questions that, at least potentially, exercise mutually contradictory influences on the eventual shape of the military organization.

Who is the likely adversary or security threat, and why do policymakers and military planners identify this adversary or threat? To begin with, the state will have to identify and, if necessary, prioritize the threats it may face in the future. However, the identity of the likely adversary or security threat to the state is problematic, because the drivers of the process through which the state's policymakers and military planners come to identify and prioritize the likely adversary or adversaries (this article proposes two principal drivers, history and geography) are at least potentially contradictory imperatives themselves.[11]

The history of the state, and especially its military history, can be illustrative of the likely potential adversaries the state may face. This history forms a key element in the complex compound that is a state's strategic culture.[12] History helps policymakers to identify the national security interests (and security policies) of the state.[13] It provides the tools with which policymakers and population can define and understand the situation they are in, interpret adversarial motives, and suggest ways and means by which state interests can be realized despite such adversarial intentions.[14] Of course, this history is much more than a purely objective reality, more than just "one damned thing after another."[15] Rather, the history of a state is also about how an objective past is interpreted and understood, in particular by the military planners and policymakers.[16] This process of interpretation, of making sense of the objective data that a state's history provides, is important because, as political psychology informs, it is central to how policymakers and military planners understand the identity of their state, and the commensurate roles and responsibilities of the state in the international arena.[17]

The historical experiences of Singapore—from the Indonesian bombing of Macdonald House on March 10, 1965, during the *Konfrontasi*, to the occasional threats by Malaysian politicians to abrogate the 1961 and 1962 water agreements between Singapore and Malaysia—point to potential threats emanating from its immediate neighbors, Malaysia and Indonesia.[18] In the case of the Indonesian bombing, when the Indonesian navy commissioned in 2014 a *Bung Tomo*-class corvette as the KRI *Usman Harun*, named after the Indonesian marines who perpetrated the Macdonald House bombing, the Singapore government was predictably upset; in the words of

Singapore Defense Minister Dr. Ng Eng Hen, this event threatened to "undo the conciliatory actions from both sides that had lain to rest this dark historical episode" and would "re-open old wounds."[19]

This leads to the following question: what are the geographic conditions of the state that have a potential impact on the latter's security calculus? There is widespread agreement among scholars of strategy that geography—both political as well as military geography—matters in shaping the threat perceptions of policymakers and military planners.[20] More often than not, it is precisely over geography that states go to war with one another. Geography provides the context, the physical location, in which strategy exists: for instance, a state with limited maritime boundaries is not going to spend much time worrying about its naval power. How do these geographic conditions influence the potential conduct of military operations by the state and its putative aggressor? Geography also influences—perhaps even drives—strategic planning and the conduct of military operations; military planners have to take into consideration the terrain of the likely conflict and the types of military capabilities needed to operate in this terrain.

However, as with a state's history, the strategic importance of a state's geography is as much an objective physical reality as it is psychologically and socially constructed. For instance, it is surely indisputable that Singapore is a small island state, yet strategically and diplomatically, Singapore might very well be anything but. To illustrate, a former Singapore Ambassador, Bilahari Kausikan, published *Singapore Is Not an Island*, a volume comprising his previous writings and public speeches as then-Permanent Secretary of the Singapore Ministry of Foreign Affairs.[21] In it, he argued that Singapore can at least mitigate against, if not escape, the strategic implications of the geographical reality that it is a small island state through adroit and robust diplomacy. In addition, a furor that erupted in 2017 involving two former ambassadors demonstrated that this objective physical reality could be interpreted very differently in strategic and diplomatic terms.[22]

Following from the above discussion, the third question to ask is: what capabilities does the state's military organization then need to defend itself against this putative adversary? However, there are two caveats to note.

The first caveat relates to what capabilities and technologies the state can acquire. Economics is only part of the picture; of course, financial costs are an important consideration, and military spending ought not to bankrupt the country's economy. Singapore's first Defense Minister, Goh Keng Swee, laid this down as a fundamental principle of Singapore's defense policy.[23] More importantly, the global geopolitics of the arms trade—who buys what capabilities from which suppliers—also matters: if a country has traditionally acquired its military capabilities from either the United States or its North Atlantic Treaty Organization (NATO) allies, there is a good chance it is because the United States and NATO had come to see that country as a valuable ally. Singapore, for instance, has almost exclusively acquired its military capabilities from the United States and NATO, or if not from NATO, at least from countries that produce military capabilities that are technologically consonant with the United States (such as the Singapore navy's acquisition of naval combat systems from Sweden, for instance). At the same time, while Singapore may overtly welcome military visits from any country, the reality is that it has hosted more visits by the U.S. military than the militaries of the former Soviet Union, Russia, or China. Its security cooperation with the United States is arguably much broader and deeper than that with any other major power.

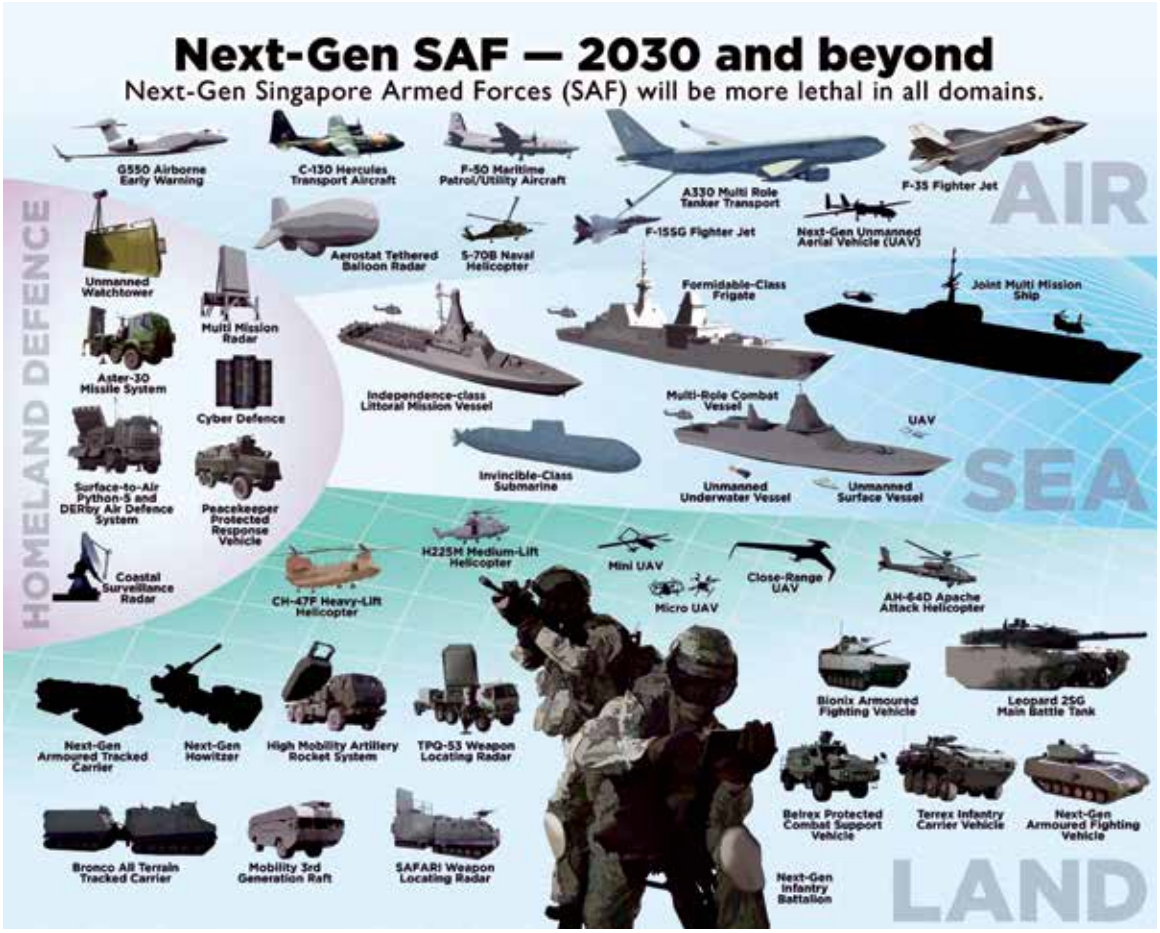
The second caveat is that there is a potential disconnect between what policymakers and military planners believe the military organization needs,

and what the military organization objectively needs (based on what it actually does). This article does not revisit the post–Cold War debates regarding the supplanting of traditional security with nontraditional security.[24] Nevertheless, I pose this question: what is the mission statement of the military organization, and what exactly does this military organization do? Since independence, Singapore has maintained a Singapore Armed Forces that was raised, sustained across three incarnations, and trained to ensure the country's sovereignty against existential threats, whether real or imagined.[25] At the same time, however, Singapore, as a sovereign state, has never had to face war; but the Singapore Armed Forces have since the 1970s participated in a number of United Nations peacekeeping operations as well as conducted a number of humanitarian assistance and disaster relief operations, from the former East Pakistan (now Bangladesh) in 1970, to its largest operation in Meulaboh in Indonesia after the December 2004 tsunami, to supporting relief operations in the United States after Hurricane Katrina in 2005 and Hurricane Harvey in 2017. The Singapore Armed Forces have also undertaken a counterterrorism mission, from the protection of critical infrastructure to the standing up of an all-volunteer high-readiness army deployment force in 2016 to address terrorist scenarios such as the attacks in Mumbai in 2008 and Paris in 2015.

It ought to be obvious that the above three questions can exercise mutually contradictory impulses on how the military organization is built. In other words, the types of military capabilities that the state acquires do not have to cohere to how the state's policymakers and military planners perceive the various threats and security challenges that the state faces. Nevertheless, as an ideal, the military organization ought to maintain a careful balance between these potentially contradictory considerations and requirements. Ideally, there will be coherence between the threats that the state faces and the types of military capabilities its military organization possesses. The operations that the military organization conducts should be consistent with the threats that the state faces. Furthermore, how this military organization is raised and sustained ought not to bankrupt the state. This is what this author understands to be a strategically coherent military organization. However, this idea of the strategically coherent military organization is also inherently problematic.

To begin with, states do not always acquire military capabilities that "make sense;" it is possible to identify cases where specific acquisitions do not necessarily cohere with the threats that the state purportedly faces. In Southeast Asia, two examples immediately come to mind: Thailand's acquisition of a helicopter carrier, and Malaysia's decision to simultaneously acquire F/A–18 and MiG–29 combat aircraft, both in the 1990s. In the first instance, it can be difficult to envision a threat scenario that Thailand might face that would require the deployment of a helicopter carrier; the carrier has only ever been deployed to support disaster relief operations. In the second instance, the acquisition of technologically incompatible combat aircraft undermines the potential for the Malaysian Air Force to operate in a cohesive manner; furthermore, this combination of Russian and American capabilities generates a logistical nightmare.

It is also worth noting that there is no such thing as an ideal answer to any of the questions and caveats identified earlier. If, as the argument here posits, there is a connection between a state's history and geography on the one hand and how the state's policymakers and military planners perceive security threats and challenges to the state on the other, it ought to be clear that neither history nor geography are singular, objective realities; rather, it is how these policymakers perceive the state's history and geography that matters. Furthermore, precisely because perceptions matter in the identification of security



Singapore Ministry of Defense
https://www.mindef.gov.sg/web/wcm/connect/mindef/be78ae40-55dd-4086-bd7a-9f893b620197/8/next-generation-saf2.jpg?MOD=AJPERES

threats and challenges, any response to any one of the questions and caveats identified above is "ideal" only to the specific policymakers and military planners of the state. In other words, it is possible to generate different and contradictory perceptions of a single objective reality. Finally, a military organization is not a static entity—hence Buzan's concept of an arms dynamic (emphasis mine). Building a military instrument is not like sculpting a statue. Rather, it is an entity that is constantly being refined, with old and obsolescent capabilities being retired, and new capabilities acquired.

Strategy, Not Lethality, Is the Key

The preceding section demonstrates that military organizations are—or at least, ought to be—assessed in terms of their strategic effectiveness—in other words, the ability of the military organization to achieve the political outcomes that the state desires. These desired outcomes can be understood in peacetime and wartime scenarios. In peacetime, the desired outcome is the maintenance of a peaceful and secure existence for the state; and in wartime, the desired outcome is the attainment of victory against its adversary. Put

bluntly, as Singapore's Ministry of Defence states as its mission, "to enhance Singapore's peace and security through deterrence and diplomacy, and should these fail, to secure a swift and decisive victory over the aggressor."

There is a strong temptation among scholars of strategy to distinguish between the twin missions of deterrence and defense. In 1946, Bernard Brodie published *The Absolute Weapon*, which was an attempt to understand the ramifications of nuclear weapons on strategy and war. In it, Brodie stated, "Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose."[26] Glenn Snyder argued that "different types of military force contribute in differing proportions to these two objectives. Deterrence does not vary directly with our capacity for fighting wars effectively and cheaply; a particular set of forces might produce strong deterrent effects and not provide a very effective denial and damage-alleviating capability. Conversely, forces effective for defense might be less potent deterrents than other forces which were less efficient for holding territory and which might involve extremely high war costs if used."[27]

However, for non-nuclear military organizations, the ability to wage and win a war against a putative enemy is central to its peacetime function of deterring adversaries from initiating hostile military operations. Deterrence holds when an adversary calculates that the costs incurred as a result of initiating military operations will be greater than the possible gains it accrues. In the nuclear realm, the issue of cost is arguably stark and unmistakable: the image of a nuclear mushroom cloud creates a powerful argument that a nuclear war produces only losers, no winners. In the non-nuclear realm, however, cost is determined by the inability of the aggressor to attain its desired end states; it is the ability to deny the aggressor its desired end states that constitutes deterrence.

There have been a number of wars where more powerful—and, presumably, more lethal—military organizations were not strategically effective. In the Korean War, more North Korean and Chinese soldiers died compared to their United Nations counterparts. Similarly, in the U.S. war in Vietnam, more North Vietnamese and Viet Cong combatants were killed in action than U.S. and South Vietnamese soldiers. As Harry Summers wrote, "On the battlefield itself, the Army was unbeatable. In engagement after engagement the forces of the Viet Cong and of the North Vietnamese Army were thrown back with terrible losses. Yet, in the end, it was North Vietnam, not the United States, that emerged victorious."[28] The pattern is repeated in more recent wars—the Soviet war in Afghanistan, the U.S.-led wars in Iraq and Afghanistan.

What these cases ought to teach us is that lethality per se does not confer strategic effectiveness. The technological superiority of one side, manifested in its superior lethality, may result in victory in battles; that being said, superior lethality does not guarantee victory in battles. If anything, these cases demonstrate a singular, if unpopular (especially in these technologically sophisticated times) truth: wars are sometimes won by stubbornness and obduracy, the sheer unwillingness to accept defeat despite battle losses, the ability to outlast the enemy, despite the enemy's technological superiority.[29] If wars are, as Clausewitz argued, a clash of mutually antithetical wills, it means that wars are decided when one side concedes. The central importance of will also, arguably, applies in peacetime deterrence—the putative adversary decides against initiating armed hostilities precisely because it does not believe that armed hostilities will allow it to realize the political interests it seeks.

Perhaps a second lesson we ought to learn is that sound strategy is necessary—although not in itself sufficient—for strategic success; arguably, it was the

absence of sound strategy that led the United States and the Soviet Union to lose its wars in Vietnam and Afghanistan, respectively. The problem is, as Colin Gray has argued, that strategy is difficult, and sound strategy can be elusive.[30]

A sound strategy requires at least three preconditions. First, it identifies a political stake involved that is unequivocally important to the national interests of the country such that the country has to resort to the use of military force. As long as the national interest at stake is clearly important, and this importance is recognized not just by the political elites but by the rest of the population as well, this provides a firm foundation for the crafting of sound strategy. Second, the country's resources will need to be mobilized to ensure that the armed forces have the necessary wherewithal to prosecute the war successfully. And there can be no half measures: no country should go to war while handicapping itself. However, as long as the national interest at stake has been clearly articulated to the population, and the population unequivocally accepts this articulation, the mobilization of resources can be achieved with a minimum of political fuss. Third, a coherent causal argument has to be constructed that relates the application of military power to the attainment of the political interests at stake. In other words, sound strategy must be able to show how the use of military power can achieve the political end states that the country seeks to establish. And sound strategy can be crafted only when political elites and military planners are involved in the process.

However, these preconditions are inherently problematic. Identifying an unequivocally important political stake in the country's national interest is challenging, if only because the policymaking community of any country is not necessarily a monolithic entity. Rather, it is composed of individuals, and the likelihood of differences in world views, philosophical biases, and opinions is almost certainly high. Within the policymaking community, it is therefore almost inevitable that there will be differences of opinions as to whether a specific political issue will constitute a core element of the country's national interests. Furthermore, the population—the source of the government's legitimacy and the country's military organization—will not necessarily agree with the opinions of the policymaking community. If there is disagreement within the policymaking community and an absence of popular support, the second precondition—the allocation and mobilization of the country's resources—will be impossible.

Finally, even if there is consensus within the policymaking community and popular agreement on the importance of the political issue, a sound strategy can be crafted only if there is agreement between the policymaking community and the military planners of the country as to how the application of military force will secure the political stakes that policymakers have identified as crucial to the country's national interest. As Colin Gray has argued, strategy is a bridge that connects policymakers and military planners.[31] Furthermore, even if all three preconditions can be met and a sound strategy is subsequently crafted, there is an additional rub: sound strategy is an essential condition for the attainment of strategic success, but it is not sufficient to guarantee strategic success. Alan Beyerchen reminds us that war is an inherently nonlinear phenomenon: the law of unintended consequences always applies, and actions will not necessarily result in the intended outcomes.[32] The combination of lethality in the form of overwhelming military power applied in a sound strategy merely increases the probability of a successful outcome. Just do not expect the lethality to get the job done.

Conclusion

When a military organization undertakes a modernization program, it is indeed expected that the new

weapons systems will be "better" than the weapons systems being replaced; it is in fact expected that the military organization, once modernized, is more lethal than its previous incarnation. Given that public money is being used to fund military modernization, and that the same public money can also be utilized in other aspects of national policy, it is indeed politically necessary that new military capabilities are better than those being retired.

However, the issue of strategic effectiveness, both in peacetime deterrence and in warfighting, is complicated. The central importance of human will in determining both the effectiveness of peacetime deterrence and victory in war means that the outcomes that military organizations seek in peacetime and in war can lie beyond the lethality of that organization. Lethal military capabilities simply do not guarantee strategic effectiveness.

Finally, the acquisition of increasingly lethal military capabilities does not guarantee that the process of military modernization will be strategically coherent. Military organizations, at least in peacetime, undertake a range of missions as dictated by the policymakers of the state, and many of these missions will not require increasing lethality. A personal anecdote illustrates this: a young Republic of Singapore Air Force pilot, who was about to begin training on the F–15SG aircraft, said to me, "If terrorist organizations are the principal security challenge facing Singapore, how am I as a F–15SG pilot going to be relevant to my organization's counterterrorism mission?" PRISM

Notes

[1] Singapore Ministry of Defence, Committee of Supply Debate 2019, March 1, 2019, available at <https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2019/cos2019>.

[2] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018).

[3] This study defines strategic effectiveness as the ability of the military organization to fulfill its peacetime and wartime objectives in support of the state's national interests. See, for instance, Bernard Fook Weng Loo, "Decisive Battle, Victory, and the Revolution in Military Affairs," *Journal of Strategic Studies* 32, no. 2 (April 2009), 189–211.

[4] *Summary of the 2018 National Defense Strategy of the United States of America*, 5.

[5] Barry Buzan, *An Introduction to Strategic Studies: Military Technology and International Politics* (Basingstoke, UK: Macmillan, 1987).

[6] *Summary of the 2018 National Defense Strategy of the United States of America*, 1.

[7] See, for instance, Max Boot, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today* (New York: Gotham Books, 2006); Martin van Creveld, *Technology and War: From 2000 BC to the Present* (New York: The Free Press, 1991).

[8] Thomas K. Adams, *The Army After Next: The First Postindustrial Army* (Palo Alto, CA: Stanford University Press, 2008), 25.

[9] *Summary of the 2018 National Defense Strategy of the United States of America*, 3.

[10] Ibid., 1.

[11] Bernard Fook Weng Loo, *Middle Powers and Accidental Wars: A Study in Conventional Strategic Stability* (Lewiston, NY: Edwin Mellen Press, 2005), 35–68.

[12] Colin S. Gray, *Modern Strategy* (New York: Oxford University Press, 1999), 131–132; Alistair Iain Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (Princeton: Princeton University Press, 1995), 35–36; David T. Twining, "Soviet Strategic Culture: The Missing Dimension," *Intelligence and National Security* 4, no. 1 (1989), 169–187.

[13] Valerie M. Hudson, ed., *Culture and Foreign Policy* (Boulder, CO: Lynne Rienner Publishers, 1997).

[14] This is illustrated by the slew of articles and newspaper editorials that attempted to portray Russia's annexation of Crimea and China's island-building operations in the South China Sea as analogous to Nazi Germany's annexation of Czechoslovakia. See "Schäuble Says Putin's Crimea Plans Reminiscent of Hitler," *Spiegel Online*, March 31, 2014, available at <http://www.spiegel.de/international/germany/schaeuble-compares-putin-moves-in-crimea-to-policies-of-hitler-a-961696.html>; "Philippine President Compares China's Expansion to Nazi Germany," *The Telegraph*, February 5, 2014 , available at <https://www.telegraph.co.uk/news/worldnews/asia/china/10618722/Philippine-president-compares-Chinas-expansion-to-Nazi-Germany.html>; "Japan PM Abe Compares China-Japan Rivalry to Pre-war UK-Germany Ties," *South China Morning Post*, January

24, 2014, available at <https://www.telegraph.co.uk/news/worldnews/asia/china/10618722/Philippine-president-compares-Chinas-expansion-to-Nazi-Germany.html>.

[15] This view of history is sometimes attributed to Henry Ford, sometimes to Arnold Toynbee.

[16] Daniel John Goldhagen, *Hitler's Willing Executioners: Ordinary Germans and the Holocaust* (London: Abacus, 1996), 28–34; Charles A. Kupchan, *The Vulnerability of Empire* (Ithaca: Cornell University Press, 1994).

[17] Hudson, *Culture and Foreign Policy*; Ronald L. Jepperson, Alexander Wendt, and Peter J. Katzenstein. "Norms, Identity, and Culture in National Security," in *The Culture of National Security: Norms and Identity in World Politics*, ed. Peter J. Katzenstein (New York: Columbia University Press, 1996), 32–75; Kupchan, *The Vulnerability of Empire*, 5–22.

[18] Tim Huxley saw Malaysia as the primary potential threat, Indonesia as the secondary; Tim Huxley, *Defending the Lion City: The Armed Forces of Singapore* (Australia: Allen and Unwin, 2000), 44–55. Also see S.R. Joey Long, "Desecuritsation and after Desecuritisation: The Water Issue in Singapore-Malaysia Relations," in *Perspectives on the Security of Singapore: The First 50 Years*, ed. Barry Desker and Ang Cheng Guan (Singapore: World Scientific/Imperial College Press, 2016), 103–120; Bilveer Singh, "Singapore's Security in the Context of Singapore-Malaysia-Indonesia Relations," in Desker and Guan, *Perspectives on the Security of Singapore*, 121–134; Yishu Zhou and Ching Leong, "Water Policies as Assets," in Critical Issues in *Asset Building in Singapore's Development*, ed. S. Vasoo and Bilveer Singh (Singapore: World Scientific, 2018), 137–148.

[19] Jermyn Chow, "Indonesian Warship Usman Harun Banned from Singapore Ports and Naval Bases," *The Straits Times*, February 18, 2014.

[20] Gray, *Modern Strategy*, 171–172; Loo, *Middle Powers and Accidental Wars*, 69–104. Also see John M. Collins, *Military Geography for Professionals and the Public* (Washington and London: Brassey's, 1998), 387–388; Roy E.H. Mellor, *National Defence: The Military Aspects of Political Geography—A Reconnaissance Study* (Aberdeen: Department of Geography, University of Aberdeen, 1987), 20–21; Patrick O'Sullivan, *Terrain and Tactics* (New York: Greenwood Press, 1991), 9–30.

[21] Bilahari Kausikan, *Singapore Is Not an Island* (Singapore: Straits Times Press, 2017).

[22] Kishore Mahbubani, then dean of the Lee Kuan Yew School of Public Policy, and a former Singapore ambassador to the United Nations, among other appointments, had published an editorial in *The Straits Times*, the Singaporean English broadsheet newspaper, on July 1, 2017, titled, "Qatar: Big Lessons for a Small Country." He argued that small states have to act with greater discretion and circumspection than their larger counterparts, and that these small states ought to pay greater attention as a result to their regional organizations and the United Nations. In response, Bilahari Kausikan, a former diplomat and permanent secretary of Singapore's Ministry of Foreign Affairs, posted a strongly worded rebuttal on his widely followed Facebook account. Bilahari's rebuttal drew favorable responses from other policymaking elites in Singapore, notably the former foreign minister and current Law and Home Affairs Minister, K. Shanmugam.

[23] Bernard F.W. Loo, "Goh Keng Swee and the Policy of Conscription," in *National Service in Singapore*, ed. Ho Shu Huang and Graham Ong-Webb (Singapore: World Scientific, 2018), 157–158.

[24] See, for instance, Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld & Nicolson, 2005); Thomas X. Hammes, *The Sling and The Stone: On War in the 21st Century* (St. Paul, MN: Zenith Press, 2004); Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era* (Cambridge: Polity Press, 1999); Charles Moskos et al., eds., *The Postmodern Military: Armed Forces after the Cold War* (Oxford: Oxford University Press, 2000); Moises Naim, "Five Wars of Globalisation," *Foreign Policy* (January/February 2003), 29–36; Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Alfred A. Knopf, 2007).

[25] Norman Vasu and Bernard F.W. Loo, "National Security and Singapore: An Assessment," in Desker and Guan, *Perspectives on the Security of Singapore*, 21–44.

[26] Bernard Brodie, *The Absolute Weapon* (New York: Harcourt Brace, 1946), 76.

[27] Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961), 4.

[28] Harry G. Summers, Jr., *On Strategy: The Vietnam War in Context* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 1981), 1.

[29] Loo, "Decisive Battle, Victory, and the Revolution in Military Affairs."

[30] Colin S. Gray, "Why Strategy Is Difficult," *Joint Force Quarterly* 22 (1999), 6–12.

[31] Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2010).

[32] Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security* 17, no. 3 (Winter 1992/1993), 59–90.

Save the date for the 7th Annual

Cyber Beacon Conference

September 9th and 10th, 2020

Marshall Hall, Historic Fort McNair, Washington, DC

* * *

Cyber Beacon is the flagship event of the
National Defense University's
College of Information and Cyberspace,
which brings together leaders, thinkers, and
practitioners to address our most pressing
information and cyberspace
national security challenges.
Prism is a proud collaborator on the effort.

cic.ndu.edu/cyberbeacon

A Small State Perspective on the Evolving Nature of Cyber Conflict

Lessons from Singapore

By Eugene E.G. Tan

Cyber conflicts among states are still largely driven by geopolitical and political considerations and should not be seen as separate from other kinds of conflict or political objectives. Brandon Valeriano, Benjamin Jensen, and Ryan Maness observe that modern cyber strategies are neither new nor revolutionary and that actions in cyberspace fall into "a domain of limited coercive actions designed to alter the balance of information as well as manage escalation risks in long-term competitive interactions." Cyber operations may offer new ways to test the robustness of networks, control messaging, or degrade a network, but they do not fundamentally change great power competition or the hierarchy of states in the international system.[1]

Small states are particularly vulnerable to the effects of cyber conflict, with larger states seeming to prefer cyber means as a way of affecting policies of the target state because of the possibility of the effects of an attack being reversed once the preferred policy of the hostile state is selected. A good example of how this happens can be seen in the 2007 Estonian cyberattack, where Russian actors sought to influence Estonian policy of moving Soviet-era statues from the city center.

Eugene E.G. Tan is an Associate Research Fellow at the Centre of Excellence for National Security of the S. Rajaratnam School of International Studies, Nanyang Technological University.

This culminated in the degradation of Estonian networks over a four-day period. While the cyberattack did not produce a change of Estonian policy, it highlighted the lengths to which states would go to affect other states' policies.

That said, the Estonian cyberattack did not cross the armed attack threshold, making an international response to the cyberattack both difficult and unprecedented.[2] To this day, states are still finding ways to address cyber conflict and are no closer to finding an acceptable mechanism to govern state behavior in cyberspace.

For the purposes of this article, the parties involved in cyber conflict are states (or state-sponsored actors) and not individuals or private corporations. That said, individuals and private corporations may still play a part in causing or exacerbating conflict by cyber means domestically and regionally or be the victims of state-led compellence measures. It is also of note that state-sponsored cyberattacks often serve a purpose and target rather than causing disparate and collateral damage to different targets, as did NotPetya.[3]

Using Singapore as the main example, this article aims to show how cyber conflict affects small states. While the means of cyber conflict may be evolving, it is still subject largely to the push and pull of geopolitical forces.

Intent to Compel

Carl von Clausewitz noted that "two different motives make men fight one another: hostile feelings and hostile intentions. Our definition is based on the latter, since it is the universal element. Even the most savage, almost instinctive, passion of hatred cannot be conceived as existing without hostile intent; but hostile intentions are often unaccompanied by any sort of hostile feelings-at least by none that predominate."[4] Using Clausewitz to understand cyber conflict may presuppose that conflict in cyberspace is in fact an act of war, but on the contrary, understanding Clausewitz well may help us understand why conflict in cyberspace will not result in cyberwar.[5] Clausewitz notes three main characteristics of war: its violent nature, its instrumental character, and its political nature.[6] Clausewitz's dictum that war is a continuation of policy by other means and the continuation of political intercourse to reach a definite goal is especially salient to the discussion on regional cyber conflict.[7] Thomas Rid's instructive piece debunking cyber war further argues that all politically motivated cyberattacks are merely sophisticated versions of sabotage, espionage and subversion.[8] Cyber conflict lacks war's violent nature but may address how it fulfills an instrumental and political purpose. Cyber conflict should therefore be understood as just one way of achieving policy goals short of war.

Internationally, in a competitive and rational situation, it is conceivable that any state will seek to use any tool, including cyber, to achieve an absolute advantage over its adversaries through a mix of deterrence and compellence. According to Thomas Schelling, there are important distinctions between deterrence and compellence as components of a coercion strategy. The main differences are in the timing and the initiative. In a compellence situation, the attacker already has accomplished the offending action, and the defender must take the initiative to respond, not just sit and wait. In other words, "The threat that compels rather than deters often requires that the punishment be administered until the other acts, rather than if he acts." In a deterrence situation, the defensive picture has already been painted. The adversary need not know the specific features of the painting, as long as no offensive act is committed. In fact, ambiguity may support deterrence. In a compellence situation, the picture must be painted for that specific situation, and it must be clear to the offender what must be done, and by when, for the victim's coercive response actions to cease.[9]

State-sponsored cyberattacks should therefore be seen in the same vein as other attacks or policy levers rather than as standalone incidents. Although the coercive effects of cyber incidents are seen as limited, the use of cyber tools is observed to complement, not replace, traditional statecraft, serving as an additive foreign policy tool.[10] The potential for regional cyber conflict should therefore not be seen as separate from other analyses of regional geopolitics.

Evolving Nature of Cyber Conflict

There are also different understandings of what cyber conflict actually entails. For decades, Western governments, practitioners, and scholars have understood cyber conflict to include protection of critical infrastructure and computer networks from hacking, or breaches of confidentiality, integrity, and availability. This understanding has been the basis of international discussions on the applicability of international law to cyber conflict, cyber norms of behavior, and deterrence of cyberattacks. The focus has been on the technology—networks, hardware, and software—instead of on the information carried by the technology.

An alternate view, led by Russia and China, has traditionally seen information as an inalienable part of cyber conflict. Russia introduced a draft resolution on information security in the First Committee of the United Nations (UN) General Assembly in 1998 and has continued to press for information security to be part of the international conversation on cyber conflict, including submitting a letter in January 2015 (together with China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan) to the UN calling for an international code of conduct for information security.[11]

While the letter was noted by the 2015 UN Group of Governmental Experts (UNGGE), the recommendations proposed by the group squarely focused on the protection of critical information and communications technology infrastructure, which was reflected in the norms proposed in the consensus report.

One reason for this focus on technology rather than information has been the philosophy of many Western democracies that any controls over the flow of information would infringe on the fundamental right to freedom of expression. Incidentally, respect for the freedom of expression, right to privacy, and other human rights was one of the norms proposed by the 2015 UNGGE.

This position appears to have shifted since the alleged Russian interference in the U.S. presidential elections in 2016. At various international conferences in 2018, including the landmark Conference on Cyber Conflict (CyCon) organized by the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, keynote speeches addressed how the use of information operations through cyber means is now an important part of cyber conflict.

Keynote speeches at CyCon 2018 by Alex Stamos (then chief security officer of Facebook) and Camille Francoise (principal researcher at Google Jigsaw) highlighted how social media is used in state-sponsored information operations, citing numerous examples of how states have used tools to influence elections and promote questionable content to destabilize incumbent governments.[12] They also called for cooperation and a common approach to misinformation and manipulation of social media. This leads to the conclusion that social media platforms need protection as much as critical infrastructure like power plants and airports.

However, including information operations in the discussion of cyber conflict is not straightforward, because the threats faced by social media platforms are different from those faced by traditional cyber targets. First, in information operations, the networks of social media platforms are not being breached but are being used for their built purpose:

spreading information. The challenge is to curb the spread of misinformation without hindering freedom of expression.

Second, information operations are designed to exploit vulnerabilities not in the technology but in the society being targeted. Tackling them requires expertise in socio-political issues, psychology, communications, and other humanities.

Third, states can build resilience to cyberattacks by constructing strong technical defenses and conducting exercises and drills. But resilience to information operations is built through institutional trust-building, media literacy education, independent fact-checking, and transparency in communication.

Fourth, while the international community has already found it difficult to develop international norms of behavior in cyber operations, where those norms only considered technology, it will be even more complex if information is included in the discussion because of states' differing philosophies on the control of information versus freedom of expression.

It can thus be said that cyber conflicts transcend the cyber domain. Potential conflicts in cyberspace may be found embedded in the broader context of information conflicts. These conflicts may take on political, economic, information, technological, media, and ideological forms in competing for influence. Targets in cyber conflict can range from key government services and institutions, internet service providers, collected personal data, or even electoral systems or media. It is therefore prudent to look for political motives to how and why cyber conflict happens to small states, how these states can choose to react to these cyber incidents, and what their limitations are.

Small States and Cyber Conflict

Small states are typically insecure about their survival and have long been the victims of great power intervention. Small states also have little recourse to both cyber and physical options for carrying out punitive action against a hostile state, with punishments being ineffective due either to scale or to the possibility of cutting off potential markets in the case of sanctions. The evolving nature of cyber conflict also means that the potential threat to small states from cyberspace no longer resides in just the physical protection of infrastructure, but also in the psychological aspects of conflict.

While Singapore is seen to be an exception to the notion of a small state because of its successful economy, advantageous strategic location, and outsized diplomatic voice, its small physical size nonetheless plays an influential role its strategic thought. In fact, Singapore, with its Smart Nation program and quest to become a data hub, has a larger cyber threat landscape than other small states, making it and its government systems more vulnerable to cyber threats made by other states.[13]

Vulnerability has been a constant theme in Singapore's foreign policy outlook since its independence, with Michael Leifer noting that Singapore, like most small states, suffers from an innate vulnerability arising from geopolitical circumstances.[14] Small states like Singapore do not have the wherewithal to carry out threats or be the aggressor because they lack the strategic depth to counter hostile actions by other states. However, while it is conceivable that small states may go rogue and use cyber means to attack a larger state (like the Sony attacks perpetrated by North Korea), these states do so in full knowledge that they have nothing to lose in not abiding by international law. Singapore, as a law-abiding international state that seeks a rules-based international order, does not have such illusions. It is well documented that Singapore employs a mix of deterrence and diplomacy to ensure its survival, and this is probably true in cyber conflict as well.[15]

As a small state, however, Singapore's ability to create deterrence against cyberattacks against

other states is very limited. For several reasons, there is limited value in pursuing classic views of deterrence through denial and punishment: technology is relatively cheap and widely available, accurately attributing blame is difficult, and identifying and punishing attackers are complex. If there is no detection or ability to punish, the credibility of deterrence by a small state like Singapore suffers.

While all states have the possibility of reacting to a cyber incident on the whole spectrum of diplomatic, information, military, economic, financial, intelligence, and law enforcement activity, small states like Singapore have limited recourse to act in the way large states like the United States or China can.[16] Small states need to be especially careful in any response because any disproportionate response to a cyberattack, which results in escalation by the attacker, could be potentially catastrophic given the vulnerability of the nation's economy, infrastructure, and physical size.

There is also a need to think about the stability in the international system should Singapore decide to pursue a deterrent strategy. The possibility of the escalation in hostilities among states is a cause for concern should a response be deemed disproportionate or inaccurate. Responses should be made when there is a clear case, rather than being based on conjecture on the potential intent of various states. Further, solely "naming and shaming" perpetrators of cyberattacks is ineffective as a response because it does not carry a strong message or have a deterrent effect. Fergus Hanson describes the Australian experience in naming and shaming the perpetrators behind WannaCry, NotPetya, and a third incident that used compromised routers for a future attack as inadequate at best and emboldening at worse. Using arson as an example, Hanson alluded that arsonists would light more fires if there were no added costs, with some relishing the added infamy of being named.[17]

In addition, there is a good chance of cyber conflicts escalating out of control should a retaliatory cycle among states take place, which will have huge implications on stability in cyberspace. The reliability of a state's commitment to enforcing its own policy statements is a significant symbol of its political and military power. If it does not retaliate or respond proportionally when a red line is crossed, it directly reduces its credibility in the eyes of the international community, undermining its ability to both intimidate and negotiate in the future. Conversely, making good on a threat in cyberspace can have drastic impacts on international stability. The full impact of an action taken in cyberspace is difficult to control or predict (for example, the spread of the Stuxnet or NotPetya malware). Therefore, retaliation may spiral beyond the intended punishment, inflicting damage over and above what would be considered a proportionate response to the breach of a threshold. This risks a minor incident triggering a tit-for-tat escalation and cascading an attack in cyberspace into a much bigger conflict. This danger is exacerbated by the risk of inadvertently punishing the wrong actor; incorrect attribution could trigger unnecessary escalation with a third party while the real aggressor goes unpunished and undeterred.

The best way for Singapore to protect its national interest vis-à-vis cyberspace is therefore by diplomatic efforts, contributing to the formation of international norms. Most norms have been agreed at international forums such as the UNGGE, in which Singapore was not a participant in the 2016–17 round. In order for Singapore to promote in detail the norms that it would like to have discussed around the world, such as the applicability of international law in cyberspace, it can do so in forums such as the Association of Southeast Asian Nations (ASEAN) Regional Forum and its various ministers' meetings and in the Shangri-La Dialogue.

In the meantime, small states should consider bolstering their domestic resilience as part of their arsenal of responses vis-à-vis conflict in cyberspace.

World Cyber Games Finals in Singapore 2005 (Conew at Polish Wikipedia https://commons.wikimedia.org/wiki/File:World_Cyber_Games,_Singapore,_2005.jpg)

Small states should prioritize the building of robust and resilient systems, which could mitigate the effects of a cyberattack. There is also a need to inoculate society against the effects of state-sponsored cyberattacks through a mix of prompt communication, proper cyber hygiene, having up-to-date systems, and quick remediation of the cyberattack. Small states should have a clear understanding of the origins of these cyber conflicts and the objectives of the aggressor state.

To do this, Singapore has proactively erected Digital Defence as the sixth pillar in its Total Defence strategy.[18] Digital Defence is a whole-of-nation effort to protect and defend the nation and secure its citizens online. It requires Singaporeans to practice good cybersecurity habits, guard against

fake news and disinformation, and consider the impact of actions performed online on the wider community. Singapore has also strengthened its legislation over disinformation online, with the Protection of Online Falsehoods and Manipulation Bill being enacted by parliament to guard against potential misuse of the internet for information conflict by other states.[19]

Capability for Cyber Conflict

That said, there are not many states around the world that have the political will, capability, and disregard for international reputation to carry out cyber operations in the areas of both information manipulation and system degradation. While an increasing number of states has expressed interest in possessing offensive cyber capacity, there is little way of knowing the level of expertise of these states. Attackers can plausibly deny responsibility for the attack, claiming that it is a false-flag operation or even that their computers have been unlawfully used to conduct an attack.[20] Conversely, attributing an attack to an innocent third party would trigger unnecessary escalation while the real aggressor goes unpunished and undeterred. The true attacker may even encourage "cascading an attack in cyberspace into a much bigger conflict."[21]

It takes a combination of technical forensics, human intelligence, signals intelligence, history, and geopolitics to identify the machine used, the specific human actor, and the entity/state that is ultimately responsible for the attack.[22] If the evidence is derived from covert intelligence operations, the state may not want to reveal its sources or capabilities.[23] It was thus prudent at the press conference following the SingHealth breach for the chief executive of the Cybersecurity Agency Singapore to state that "there are only a few countries in the world who have shown this level of sophistication when it comes to cyberattacks. . . . We are not able to reveal more because of operational security reasons."[24] As a responsible state of good repute, Singapore has not used its cyber capabilities offensively.

There is therefore a pressing need, as Clausewitz noted, to look at the intentions of the offending state. Max Smeets and Herbert Lin observed that the possession of offensive cyber capabilities is not effective in deterring other states from taking adversary military action unless a state possesses a credible threat. Offensive cyber capabilities, however, are observed to play a larger role in compellence because the effects of offensive cyber capabilities are, first, reversible, and second, do not have to be disclosed. Smeets and Lin also note that there are two points to assess if coercion is taking place: first, that the attacker may not make explicit, but implicit, demands owing to the longstanding relationships among states; and second, the demands will not explicitly spell out where the threat is going to materialize.[25] Smeets and Lin thus lay out a set of questions that states that are being coerced should ask in cyber conflict:

- What are the cyber capabilities a rival state has demonstrated, or what are the cyber trends that should be tracked?
- What is the broader context of the cyber conflict?
- Has the state been subject to longstanding demands?[26]

Singapore and the Region

According to the 2017 Australian Strategic Policy Institute Cyber Maturity Report, the Asia-Pacific region has so far escaped a major state-led cyber incident more because of the peaceful macro environment than because of strong defenses and resiliency. At the individual level, more than 55 percent of people in the Asia-Pacific are still not connected to the internet. While this represents a massive growth opportunity, it also points toward large-scale early user vulnerability as this population comes online.[27]

As a small state that seeks to be a friend to all but an enemy of none, it is probable that Singapore will not employ tools of coercion to advance its interests. This is especially so for Singapore's immediate neighbourhood, where peace and stability in Southeast Asia are absolutely essential. Consequently, Singapore as a founding member of ASEAN remains a strong advocate of the association's unity and centrality.[28]

There are two main documents that have largely contributed to the peaceful regional order in Southeast Asia: the declaration of the Zone of Peace, Freedom, and Neutrality, and the Treaty of Amity and Cooperation. Relations among ASEAN member states have been generally stable, and with the exception of the Thai-Cambodian border dispute, there has been no armed conflict among the ASEAN member states.[29] There have been other minor arguments between ASEAN member states, but these have not crossed the threshold where war or direct conflict is the automatic extension of government policy.

This is not an indication that cyber conflicts will not happen in ASEAN, but merely an indication that member states have not resorted to cyber operations to influence policies. Further, it is perhaps fortunate that because ASEAN member states are not as developed in terms of cyber capabilities, conflicts among them in the physical domain have not evolved into cyber degradation exercises.

That said, apart from the gaps in capability, ASEAN has been doing much in cyber diplomacy to stave off cyber conflicts. In 2018, ASEAN member states sought to advance the operationalization of cyber norms in the region. The 32nd ASEAN summit in April 2018 brought on a slew of statements from leaders recognizing that norms and the rule of law are needed for cyberspace and as a basis for using technology to advance economic growth in the region.[30]

The ASEAN Leaders' Statement on Cybersecurity made at the summit called for the identification of a concrete list of voluntary, practical norms of state behavior in cyberspace that ASEAN can work toward adopting, taking reference from the 11 norms recommended by the 2015 UNGGE.[31]

The ASEAN Ministerial Conference on Cybersecurity (AMCC) held in September 2018 also agreed that there is a need for a more formalized mechanism for ASEAN cyber coordination and has tasked Singapore to propose a mechanism for the AMCC to consider. The AMCC also has agreed in principle to subscribe to the 11 voluntary, nonbinding norms recommended by the 2015 UNGGE, as well as to focus on regional capacity building in implementing these norms.[32]

Singapore and Extra-Regional Conflict

Cyber conflicts are not limited by region, as can be seen by the Stuxnet and Shamoon cyberattacks inflicted on Iran and Saudi Arabia respectively. Southeast Asia is a confluence point for great power competition, with an increasingly assertive China and a still interested United States each emphasizing its role in the region.

Flashpoints have resulted in offensive cyber capabilities being used to signal displeasure and compel and coerce some states in the region to heel. For example, it is widely speculated that China was behind a series of distributed denial of service attacks on the Philippines after the Permanent Court of Arbitration ruling dismissing China's claim of ownership of the South China Sea. The attacks began almost as soon as the verdict was released on July 12, 2016, and targeted key Philippine government agencies including the Department of Foreign Affairs, the Department of National Defense, the Central Bank, and the Presidential Management Staff. Similarly, Vietnam has been targeted by Chinese cyber units because of its South China Sea position, particularly after an incident over a Chinese oil rig in Vietnamese-claimed waters in May 2014. In this instance, Vietnamese intelligence networks were

compromised by Chinese hackers, leaking sensitive information over Vietnam's diplomatic and military strategy.[33]

With the superpowers and other regional powers, Singapore's aim is to expand its relationships, both politically and economically, to remain relevant and ensure that it is in the best interests of other states that Singapore continues being successful. This delicate balancing act is easier in good and peaceful times, but obviously more difficult when superpowers and regional powers contend with one another, such as the power competition and trade war between the United States and China. Nevertheless, Singapore aims for balance and promotion of an inclusive architecture. Singapore fastidiously avoids taking sides in great power conflict, refusing to side with one side against another. While Singapore spares no effort to develop a wide network of relations, these relations must be based on mutual respect for each other's sovereignty and the equality of nation states, regardless of size. Diplomacy is not about just having "friendly" relations at all costs, but about promoting friendly relations as a way to protect and advancing Singapore's important interests.[34]

Singapore's uncompromising but principled stance when rivals make unreasonable demands that hurt or compromise its national interests may cause friction with the great powers in the region. A good example of this is the impounding of Singapore's armored personnel carriers in Hong Kong in December 2016 as one way that Beijing signaled displeasure toward Singapore for its stance on the affirmation of international law on the South China Sea issue.[35] While China has in this instance used a physical lever to pressure Singapore to change its stance, China is well capable of using its huge offensive cyber capability for similar reasons. China has also demonstrated its capability and willingness to use information warfare tactics on other states such as Taiwan.[36]

Other states with vested interests in the region have declared their offensive cyber capabilities and have shown a willingness to use these capabilities. Australia, for one, announced that it has used its offensive cyber capabilities to degrade the Islamic State's command and control networks.[37] The United Kingdom has also announced that it will set up a 250-million-pound cyber taskforce to combat Russian and terrorist aggression in the wake of the Novichok chemical attack in Salisbury.[38] The United States has announced that it has authorized the use of offensive cyber operations against adversaries to protect its interests without specifying how these will be used or what behavior it will seek to coerce.[39] The possibility of extra-regional conflict is therefore high and may inadvertently affect Singapore and the other states in the Southeast Asian region both domestically and internationally.

Domestic Implications of Cyber Conflict for Singapore

Michael Raska notes that because cyber-enabled conflicts increasingly challenge traditional boundaries between peacetime and wartime, geography and distance, state and non-state actors, and civil and military domains, Singapore's defense strategy has to correspondingly adapt to the challenges emanating from cyberspace.[40] As the international community begins to recognize information operations as part of cyber conflict, states such as Singapore will have to develop new policies and possibly even new organizations to respond to information operations alongside the more traditional cyber security challenges. This may include the development of doctrines or framing of appropriate and proportionate responses to cyber incidents.

The SingHealth cyberattacks of 2018 also show that public confidence can be easily shaken or affected by a cyberattack.[41] In order to mitigate the impact of cyberattacks that aim to destabilize or demoralize society, Singapore needs to build

resilience through public education and public drills and exercises. At the community level, Singapore can build cyber resilience by training to respond to attacks, similar to fire drills and emergency drills held today. At the industry level, businesses can build resilience by training to respond to breaches and by maintaining backup systems that can be called upon in times of emergency. At the state level, the government plays the key role of chief coordinator to encourage the development of resilience within society toward these new national security challenges.[42]

Information operations can also pose a threat to society and should be considered as part of cyber conflict. Some of the information fed to cyberspace is fabricated or manipulated to help hostile states achieve a certain policy objective. To better understand this phenomenon, the Parliament of Singapore convened a Select Committee on Deliberate Online Falsehoods, calling upon international experts and tech companies to testify about the effects of deliberate online falsehoods. The report of the committee has provided 22 recommendations for responding to them. These new policies and organizations will need expertise in a range of areas such as strategic communication, public education, fact checking, and international relations.[43] Cyber conflict will continue to evolve at a rapid rate, and states will need to produce timely and effective measures to prevent and combat the effects of these conflicts.

International Implications of Cyber Conflict for Singapore

Currently, because of the lack of international agreements and laws, coupled with the weak enforcement of norms regarding cyberspace, cyber conflict is largely ungoverned. The inability of the 2017 UNGGE to agree on how international law applies in cyberspace may lead states to conclude that there are few, if any, rules in cyberspace, and increase the risk of cyber conflict.

The absence of a normative regime in cyberspace at the moment allows malicious actors to operate in a grey area where there is a low-risk, high-reward scenario to the attackers. In a sense, states are bound in a no-win situation where the strong do what they want, and the weak suffer what they must in world without norms.

Establishing norms in cyberspace, however, is not a straightforward process. The recent shift in global power politics means that states with revisionist ambitions are emboldened to challenge the existing international order. The United States' unipolar moment is giving way to a multipolar world, and that has serious implications for the survival of today's international norms. China and Russia are both challenging accepted norms in political, military, and economic arenas, testing the limits of the status quo. The relative "newness" of cyberspace makes it more malleable than other traditional domains that have set legal and normative frameworks.

Norms should preferably be applied to all states, but seeking narrow consensus with a few dialogue partners may help shape norms globally. Following the impasse at the 2017 UNGGE, China is pushing for a regional ASEAN cyber security agreement that leaves out the United States.[44] This is consistent with China's foreign policy of engaging with global institutions on its terms and mirrors what China is doing geopolitically in the region, which is to frame the United States as an outsider that should not meddle in regional matters or strategic thinking. This point of dividing ASEAN in favor of bilateral negotiations should not be taken lightly especially when a strong consensus over norms for cyberspace is needed.

One of Singapore's foreign policy principles is to promote a global world order governed by the rule of law and international norms. Norms are especially important to small states like Singapore, as norms set out the rights of states, including the protection of critical infrastructure from malicious attacks,

noninterference in political processes, and the illegality of economic espionage. In a system where "might is right" or the laws of the jungle prevail, small states like Singapore have very little chance of survival. The international order is strengthened by the safeguarding of the rights and sovereignty of all states and the rule of law. Great powers will still have more influence and say, but they do not get a free pass to do as they please.

The pace at which international law is being made is slow and may at times incur headwinds that are insurmountable. For example, while the 2012–13 round of the UNGGE agreed that international law applied to cyberspace, the 2016–17 round failed to agree on how international law applies to cyberspace.[45] International law will thus take a long time to formulate, and it may be a while before states can agree on an international law regime.

But the creation of a rules-based order is one of the ten key principles underscoring the Leaders' Vision statement and calls upon ASEAN to promote the rule of law, anchored in respect for international law and norms. This will in turn help with the development of the ASEAN Smart Nation network and fulfil the leaders' pledge on cybersecurity cooperation.[46] While this may seem like a small step for most other regional organizations, the differences in the capacity and understanding of the ASEAN states is not to be and should not be conflated with the needs, interests, and wants of the individual Southeast Asian states. That is why the Leaders' Vision statement agreed at the ASEAN Summit in April 2018 is significant and should be lauded as a good piece of diplomacy.

An agreed set of norms will benefit and affect all states in the international system, even those that have chosen not to adhere to the norms regime. States may be deterred from flagrantly ignoring the regime because of the risk of reputational loss. Singapore strives to be part of this conversation and is a participant in the Open-ended Working Group and the UN Group of Governmental Experts. These two groups will meet in the upcoming months, and it is imperative that Singapore, through its representation at the UNGGE, represents how small states need to be protected by international law and norms.[47]

Finally, since cyber conflict does not respect borders, there is an urgent need for states to formulate rules or laws to govern international relations in cyberspace. All small states like Singapore should be proactive in participating in norms discussions globally to create a rules-based order for cyberspace and seek to prevent cyber conflict globally lest larger states run roughshod over the interests of smaller states in cyberspace. PRISM

Notes

[1] Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018), 5.

[2] "How a Cyber Attack Transformed Estonia," BBC News, April 27, 2017, available at <www.bbc.com/news/39655415>.

[3] "Petya: Is It Ransomware or Cyberwarfare?" CSO Online, June 29, 2017, available at <www.csoonline.com/article/3204508/petya-is-it-ransomware-or-cyberwarfare.html>.

[4] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 75–77.

[5] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

[6] Clausewitz, *On War.*

[7] Ibid.

[8] Rid, "Cyber War Will Not Take Place."

[9] Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

[10] Valeriano, Jensen and Maness, *Cyber Strategy*, 3.

[11] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, July 22, 2015.

[12] "CyCon 2018 Video: Current and Former Presidents, NATO and Facebook Experts," *ERR News*, May 31, 2018, available at <https://news.err.ee/836012/cycon-2018-video-current-and-former-presidents-nato-and-facebook-experts>.

[13] Cyber Security Agency Singapore, *Singapore Cyber Landscape 2018* (Singapore: Cyber Security Agency

Singapore, 2019).

[14] Michael Leifer, *Singapore's Foreign Policy: Coping with Vulnerability* (New York: Routledge, 2000, 10.

[15] "Singapore's Poison-shrimp Defence," *South China Morning Post*, February 6, 2004, available at <www.scmp.com/article/443461/singapores-poison-shrimp-defence>.

[16] Jelle van Haaster, "Assessing Cyber Power," in *8th International Conference on Cyber Conflict: Cyber Power*, ed. Nicolaos Pissanidis et al. (Tallinn, Estonia: NATO CCDCOE, 2016).

[17] Fergus Hanson, "Naming and Shaming the Unshamable," *The Strategist*, April 16, 2018, available at <www.aspistrategist.org.au/naming-shaming-unshameable/>.

[18] The other five pillars of Total Defence are military, civil, economic, social, and psychological defense. Ministry of Defence Singapore, "Fact Sheet: Digital Defence," available at <www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2019/February/15feb19_fs>.

[19] Government of Singapore, *Protection from Online Falsehoods and Manipulation Bill*, Bill No. 10/2019, available at <https://sso.agc.gov.sg/Bills-Supp/10-2019/Published/20190401?DocDate=20190401>.

[20] Kenneth Geers, "The Challenge of Cyber Attack Deterrence," *Computer Law and Security Review* 26, no. 3 (2010): 301.

[21] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2013), 137.

[22] Herbert Lin, "Attribution of Malicious Cyber Incidents," *National Security, Technology, and Law*, 2016, available at <www.hoover.org/sites/default/files/research/docs/lin_webready.pdf>; also, Sean Kanuck, former U.S. National Intelligence Officer, in closed-door roundtable with CENS/RSIS in September 2018

[23] Delbert Tran, "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack," *Yale Journal of Law and Technology* 20, 376.

[24] Aqil Haziq Mahmud, "SingHealth Cyberattack: What You Need to Know," *Channel News Asia*, July 20, 2018, available at <www.channelnewsasia.com/news/singapore/singhealth-cyberattack-what-you-need-to-know-10549096>.

[25] Max Smeets and Herbert S. Lin, "Offensive Cyber Capabilities: To What Ends?" in *2018 10th International Conference on Cyber Conflict Cycon X: Maximising Effects*, ed. T. Minarik, R. Jakschis, and L. Lindstrom (Tallinn, Estonia: CCDCOE, 2018), 55–88.

[26] Ibid.

[27] Australian Strategic Policy Institute, *Cyber Maturity in the Asia-Pacific Region 2017* (Canberra, Australia: ASPI, 2017), available at <www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017>.

[28] "Full Speech: Five Core Principles of Singapore's Foreign Policy," *Straits Times*, July 17, 2017, available at <www.straitstimes.com/singapore/five-core-principles-of-singapores-foreign-policy>.

[29] "Ruling Doesn't Quell Thai-Cambodia Border Row," *Al-Jazeera*, November 13, 2013, available at <www.aljazeera.com/indepth/features/2013/11/ruling-doesn-quell-thai-cambodia-border-row-201311131220753174 7.html>.

[30] ASEAN, "ASEAN Leaders' Vision for a Resilient and Innovative ASEAN," available at <https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Vision-for-a-Resilient-and-Innovative-ASEAN.pdf>.

[31] ASEAN, "ASEAN Leaders' Statement on Cybersecurity Cooperation," available at <https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf>.

[32] Cyber Security Agency Singapore, "ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts," available at <www.csa.gov.sg/news/press-releases/amcc-2018#sthash.ZV7PZrTI.dpuf>.

[33] Anni Piiparinen, "China's Secret Weapon in the South China Sea: Cyber Attacks," *The Diplomat*, July 22, 2016, available at <https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/>.

[34] "Full Speech: Five Core Principles of Singapore's Foreign Policy."

[35] "How Singapore's Military Vehicles Became Beijing's Diplomatic Weapon," *South China Morning Post*, December 3, 2016, available at <www.scmp.com/week-asia/politics/article/2051322/how-singapores-military-vehicles-became-beijings-diplomatic>.

[36] Gulizar Haciyakupoglu and Benjamin Ang, "Civilians in the Information Operations Battlefront: China's Information Operations in the Taiwan Straits," in *DRUMS: Distortions, Rumours, Untruths, Misinformation, and Smears*, ed. Norman Vasu, Benjamin Ang, and Shashi Jayakumar (Singapore: World Scientific, 2019), 83–113.

[37] "Australian Cyber Intelligence Agents Helped Defeat IS," *9 News*, March 27, 2019, available at <www.9news.com.au/national/national-news-australian-cyber-intelligence-agents-helped-defeat-is/527d8b63-cd82-4e0e-ba8a-b2116074eeff>.

[38] "May Vows Revenge on Russia over Salisbury Novichok Poisonings," *The Times*, September 6, 2018, available at <www.thetimes.co.uk/edition/news/may-vows-revenge-on-russia-over-salisbury-novichok-poisonings-93lk85sjr?utm_campaign=Echobox-&utm_medium=Social&utm_source=Twitter#Echobox=1536215469>; "Britain Steps Up Cyber Offensive

with New £250m Unit to Take on Russia and Terrorists," *The Telegraph*, September 21, 2018, available at <www.telegraph.co.uk/news/2018/09/21/britain-steps-cyber-offensive-new-250m-unit-take-russia-terrorists/>.

[39] "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *Washington Post*, September 20, 2018.

[40] Michael Raska, "Cyber Conflicts and Singapore's 'Total Defence' Strategy," *RSIS Commentary*, June 23, 2016.

[41] Government of Singapore, *Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018* (Singapore: Government of Singapore, January 10, 2019), available at <www.mci.gov.sg/coireport>.

[42] Norman Vasu and Benjamin Ang, "Embracing Technology to Boost National Security," TODAY, December 22, 2016, available at <www.todayonline.com/technology-0/embracing-technology-boost-national-security>.

[43] Parliament of Singapore, *Report of the Select Committee on Deliberate Online Falsehoods—Causes, Consequences, and Countermeasures* (Singapore: Government of Singapore, 2018).

[44] Valeriano, Jensen, and Maness, *Cyber Strategy*, 170.

[45] Eugene E.G. Tan, "The Challenge of Getting Responsible Behaviour in Cyberspace," *RSIS Commentary*, October 6, 2017.

[46] ASEAN, "ASEAN Leaders' Vision for a Resilient and Innovative ASEAN," and "ASEAN Leaders' Statement on Cybersecurity Cooperation."

[47] United Nations, "First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct," GA/DIS/3619, November 8, 2018, available at <www.un.org/press/en/2018/gadis3619.doc.htm>.

"Thinking About What Could Be"

An Interview with General John M. Murray, Commanding General Army Futures Command

What were the circumstances that led to the creation of Army Futures Command? In other words, what is the problem that the creation of the new command is the solution to?

Army Futures Command is an adaptation to the on-going change in the international order we have seen since the end of World War Two. The rules of the road for international order have changed; Russian destabilization of Ukraine, Chinese assertiveness in the South China Sea, and the inevitable shift from an Atlantic-based global economy to a Pacific-based economy.

Russia and China watched the American way of war, first in Operation *Desert Storm* and then in the opening phases of Operation *Iraqi Freedom*, and fundamentally decided that close combat with the United States and our allies was not a winning proposition. Their concept of layered standoff—which we think is fundamental to their theory of victory—beginning below the threshold of war, sees constant competition below that threshold. We have seen it in Ukraine, the South China Sea, and the Baltics; all attempting to achieve strategic objectives below the threshold of war.

In western society we tend to see long periods of peace interrupted by short periods of war as the norm, while many of our adversaries see the world in constant competition—not necessarily always military, but through all the elements of national power; diplomatic, information, economics, as well as military. That's a different kind of world perspective; but from a U.S. Army perspective, our almost singular focus on counterinsurgency for the last 18 years—which was exactly what was needed when you are losing soldiers each and every day on those battlefields—cost us an entire generation of modernization. We also suffered some pretty large failures in developmental programs; Crusader, Comanche, and Future Combat Systems, which basically means that we are fighting today with the same platforms we fought with when I was a company commander back in the

Interviewed by PRISM Editor-In-Chief Michael Miklaucic on November 5, 2019

mid-1980s. They have different capabilities now because they have been upgraded over time, but the fact remains that the architecture is the same; the physics that went into building the Abrams and the Bradley are 40 year old technologies.

These were the big things that contributed to the Army's decision to modernize; and the four most senior Army leaders—the Army Chief of Staff, the Secretary of the Army, the Undersecretary, and the Vice Chief of Staff—were in unison in their visions of what the Army needed to do and how we were going to do it. Specifically regarding the Army Futures Command, General Mark Milley at that time looked at the enterprise called the Army and saw there was really nobody focused on modernization; all focused on the short term with nobody looking deep into the future to figure out what the future operational environment might look like. Nobody was anticipating the next operating concepts inside that environment, and nobody was looking at what had to be developed to succeed.

Modernization is a continuous process requiring collaboration across the entire Army. Army Futures Command (AFC) under the direction of Headquarters, Department of the Army, brings unity of effort to the Army's modernization approach by developing and delivering future concepts, requirements, and organizational designs based on its assessment of the future operating environment. Before AFC, the first place modernization was synchronized was at the Chiefs and Secretary of the Army level. That lack of unity of effort and unity of command, that lack of a command focused on the future and what the future challenges might be—beyond material—and the need to orchestrate the effort is really what led to the establishment of the Army Futures Command.

How has the Command been stood up?

It started off as a task force: we uncased the colors here in Austin in August 2018, so we are 14 months old. Across the entire command we have gone from about 40 to 26,000 personnel; here in Austin we have about 400 on the ground, and a requirement for another 100. We have limited direct hiring authority, but not every position can be a direct hire, so most hires go through the normal hiring process.

How does the Command select and prioritize its initiatives and its research?

One of the things I have learned over the past year is to clearly identify the challenges or problems we are trying to solve. There is a lot of great research that goes on in military laboratories, in the Army, Air Force, Navy, Marine Corps, as well as great research in universities; and lots of great innovation all over this country. But if you are out there searching for great technologies and then trying to find a problem for them, that is actually the reverse of how it should be done. So we have spent the last 6 to 8 months focused carefully on identifying the technological challenges or problems that our cross-functional teams are working on or need solutions to. We will soon bring all the program executive officers together to focus directly on their major problems from a technology standpoint, or a research and development, or science and technology standpoint. We then focus the Army Applications Lab— as well as our internal laboratories—on solving those problems. Identifying the problems first before you go and try and find the solutions, as opposed to vice versa.

How does the Command actually go about identifying those problems?

We sit down with each of the cross-functional teams and ask them to step beyond what they are currently working on and start to figure out what comes next. Some of the coming challenges—take, for example quantum; quantum is not here yet, but it is coming sooner or later. The Artificial Intelligence Task Force, embedded at Carnegie Mellon University and partnered with leading researchers across the country, is defining and developing future capabilities

for AI-enabled Multi-Domain Operations in order to think through the impacts of AI on a future battlefield. Not unique to the military, but pretty much across the military—especially the Army—we tend to think in terms of what is, as opposed to what could be. So we try to shape our thinking about what could be, and how emerging technologies that may not be here yet, but are coming, could fundamentally change the way we fight.

How does the Command interact with academia and the private sector that is different than the way the Army has traditionally interacted with those communities?

We have invested in universities for a long time and invested in university research. We had a small business program for a long time, but it is the laser focus we are able to bring by understanding the problems we are trying to solve upfront. We currently have three strategic university partners: one of them is focused on hypersonic and directed energy; another is focused on robotics and autonomy and precision navigation and timing, so that in a degraded environment you can still ensure navigation and timing; and a third partner is focused on Artificial Intelligence. These are the things we are currently focusing on. It is the focus on specific challenges that distinguishes our approach to academe and the private sector.

The data base of problems we are currently addressing—around 40 at this time, and it will continue expanding—is open to private industry as well. In our public communications we lay out our problems and invite companies from across the country, small, medium, and large, to come hear us, and focus on the problems we are trying to solve.

Does Army Futures Command work closely with the Defense innovation unit?

The Defense Innovation Unit has an office in Austin making Austin a hub. We have the Air Force Innovation Unit, the Defense Innovation Unit, Army Applications Lab, and National Geospatial Agency all located in the same building, so the hand off of problems, technologies, and solutions happens all the time.

How do the cross-functional teams operate? How are they composed? How are they given their assignments? Do they interact with each other?

They interact with each other constantly. Something we have done poorly in the past is communicate across systems; every system operates as a part of a bigger system. The whole is an integrated system of systems construct. Take for example a cannon I want to develop that shoots 1000 miles; if I can't see 1000 miles, and I can't pass targeting data back to that cannon in near real time, and I can't do battlefield damage assessment of those fires, then that cannon that shoots 1000 miles is interesting, but not very relevant. Looking across the cross-functional teams is a systems approach to how all the systems interact together and about how they all have to communicate together. That drives integration across the cross-functional teams almost from inception.

Cross-functional teams include operators, scientists, engineers, testers, costers, requirements experts, acquisitions experts. The theory behind them is if you get the team together in the beginning with a better set of products that drive the development of a capability, you end up with better early prototypes to drive the requirements; you end up with better prototyping so you don't have to go through a constant changing of requirements through the lifecyle of a program. The most powerful thing about the cross-functional teams is the partnership between the program manager, and the cross-functional team director, all sitting around the same table focused on the same problems every day, focused on the same outcomes, without VTCs, phone calls, and TDYs. This is one of the most powerful lessons we learned during the first year.

How do you anticipate our peer competitors' intentions and capabilities?

This is not easy, and it is not perfect. We start with the attitude that we are not going to be exactly right, and that's okay. I fundamentally believe there has to be some goal or objective you are after in the future, or else any road will get you there. We have a directorate of Intelligence that is different than any other intelligence directorate I have ever been associated with that has a distinctly Army Futures Command perspective. We are not at all interested in what is happening today, or next year, or the year after that. We have a very small group of people trying to harness the power of the entire Intelligence Community, to make predictions well into the future. First of all is understanding. It does not matter who our adversary is; we must understand where they currently are, understand from a lot of open source inputs about what their intentions appear to be, and then ground that with the technology forecasting expertise we have to anticipate what path they are on. Then we can establish what they say they want to do, where they currently are, and what path we think they will take to get there. There will be some key points over time that either prove or disprove that those technologies are imminant; and we focus on getting there ahead of our adversaries to establish overmatch. We do not want to get to 2035 to find we have fallen behind. We want to aim ahead of the competition and not behind it. Understanding the technology paths, understanding the feasibility of what they are trying to do, the technological hurdles they will have to overcome to get there, and from an intelligence standpoint, we must establish information requirements so we can begin to track them

What in your view is a possible, a credible scenario in which the Army would confront peer competitor armed forces?

I believe the greatest vindication of Army Futures Command would be that that day never comes. This is, and has always been, about deterrence; it will always be about deterrence. The goal is not to win the future conflict, but to never get into a future conflict. It is hard to predict what might lead us into a major conflict. I don't think anybody predicted the assassination that led to World War I. When the Allies were negotiating with Hitler, very few predicted World War II, or Pearl Harbor. It could be any one of a thousand events that could get us there. But the primary goal has always and remains deterring war.

Isn't that what we believe the Chinese and Russians are thinking as well? They are trying to out maneuver us—to defeat us—without having to confront us militarily?

In a different way, they are achieving many of their strategic objectives below the threshold of war. You can call that grey zone conflict with little green men, you can call that whatever you want to call that. As I said earlier we embrace a very western concept of long periods of peace as the norm, punctuated by short periods of war, whereas most of our adversaries see constant competition, not just from a military stand point; diplomatic, the information space, and as long as they can continue to achieve objectives below the threshold of outright war, what is needed is a whole of government effort to counter it.

Does that lead you to believe the United States should adopt or embrace that kind of world view of persistent competition?

The first step is recognizing that we are in a state of competition, and there are events happening that are making people slowly realize what is happening, primarily through the information space, the diplomatic space, and the economic space. Economics has always been a great power tool.

Based on your experience here with the Army Future Command, what recommendations can

you make for joint professional military education? What insights do you have from this Command that we should be taking into consideration in developing the next generation of JPME?

As I reflect on my professional military education experiences and recall how much time we actually spent thinking about the future, the answer is not very much, if any. We don't spend any time in JPME, thinking about things like quantum; but quantum is coming. A lot of things out there are coming; it's not a question of if. People are scared to death of Artificial Intelligence on the battlefield, imagining The Terminator; but there are so many applications of Artificial Intelligence well short of killing machines, that would be very effective. Despite our fears, our ethical considerations, and the debates that go on, Artificial Intelligence and quantum will come to the battlefield. I didn't spend any time at all in my professional military education thinking not about what is, but about what could be. Yet, thinking about what could be is important if we are trying to reverse engineer things back to what we need to focus our research and development, our science and technology on. Innovation for innovation's sake is interesting, but focused innovation is more important than just innovating for the sake of innovation.

Do you consider that important for the next generation of national security leaders? To be learning to think like that?

The Army undervalues that type of strategic thinking; we undervalue some of the foreward looking skill sets. Yet, General McConville—the Chief of Staff of the Army—has said on numerous occasions that you cannot be an analog army in a digital age. But if we are truly going to move into the digital age, it is skill sets like the emerging field of Artificial Intelligence engineering, computer science, and data science that we must develop. Not that we need thousands and thousands of data scientists, but we are going to need some people to help us move into the information age. The Army is trying. We went through this with the cyber workforce 10 years ago; how do you recruit and then retain a very talented cyber work force? And we will have to do the same with some other non-traditional skill sets.

What kind of insights from your experience here at Army Futures Command would you share with the next generation of national security leaders, the graduates of National Defense University?

I had the advantage of coming into the Army post-Vietnam in the all-volunteer Army and was shaped very early in my career by Airland Battle Doctrine. I went to the captain career course at Fort Benning and it was focused on the emerging doctrine. I spent some time at the National Training Center focused on decisive action training and then returned to Fort Benning and taught Airland Battle. For good reasons, over the last eighteen years, we lost that focus on theory and doctrine and concepts as we have focused almost singularly on a counterinsurgency fight. We cannot lose what we have learned over the last eighteen years. That is one of the lessons of Vietnam; we wished away that problem when we came out of Vietnam.

We cannot afford to wish away low intensity counterinsurgency; it will have to be accounted for in the next iteration of doctrine. We tend to want to focus on that high end fight, and educationally we are going back to that. At the combat training centers we are getting back where we were at the beginning of my career; focused on a near peer fight. We must account for the most dangerous scenarios, and this is happening. For the company commanders education really matters; not just education in a formal setting, but constant self-education, studying some of the things I've talked about, and thinking about some of the things I've talked about. We have been on auto pilot for the last eighteen years. That certainty is gone and we

must prepare ourselves mentally and physically for a wide variety of what could be.

You mentioned the fact that we have been focused on counterinsurgency for the last eighteen years and it's a little bit of a rerun of Vietnam; it seems we are pulling back from those kinds of operations and already a lot of the complex operations centers are closing down replaced by new cyber and AI centers. How do we avoid that same process of forgetting.

I am convinced personally and professionally that we will be involved in counterinsurgency for decades, because many of the root causes of insurgency have not been addressed over the last eighteen years. The Army is standing up Security Force Assistance Brigades that have a counter-insurgency mission. They focus on advising and assisting our partners, and working by, with, and through partners and allies, which will help us retain some of those lessons. The Security Force Assistance Academy at Fort Benning will be be the center where most of that knowledge is going to be retained. When multi-domain operations–which is still a concept—becomes doctrine, it will have to account for that modality of warfare. I think world events are going to keep us current on counterinsurgency for the foreseeable future. PRISM

The Future of Leadership: Rise of Automation, Robotics, and Artificial Intelligence

By Brigette Tasha Hyacinth
MBA Caribbean Organisation, 2017
296 pp. $27.00
ISBN: 978-9-76960-921-1

Reviewed By Dr. Ronald Sanders

It seems like we are continuously bombarded with prophecies about how Artificial Intelligence (AI) and all of its permutations—from quantum computing and machine learning to RPA and Skynet—will radically change just about everything we do.[1] However, much of its potential (whether as promise or pariah) remains prospective, more speculative than real.

That is especially true with regard to the impact of AI on organizations and those who lead them, and given the title of Brigette Hyacinth's work, *The Future of Leadership: The Rise of Automation, Robotics, and Artificial Intelligence*, this reviewer was hopeful that it would contribute more to the discussion. Unfortunately, while it lays a foundation for that discussion, it does little to further it, especially for those who must lead in the public sphere.

The book itself has three main parts, ostensibly connected by the challenges of AI and what to do about it. The first part is an extensive catalog of those challenges, with the author opting for breadth rather than depth. Thus, the reader is treated to list after list of AI applications, ranging from the way we work (and work out) to the way we drive and eat and sleep. In so doing, the author proffers a paradox; that is, that this particular technology—like so many others—is very much a "two-edged" sword, making lives easier but bringing with it threats anticipated and otherwise.

And when it comes down to where AI falls on that promise-to-peril continuum, the author is clearly on the "Danger, Will Robinson!" end of the scale. Thus, despite chronicling all the benefits of AI, she predicts that it will ultimately cause the massive (indeed, historic) displacement of people as its principal consequence, with many millions of us left without meaningful work, our hard-earned skills and education rendered obsolete by faceless governments and corporations looking to cut costs at all cost.

I have a different, less pessimistic view; that is, that we will muddle through . . . that technologies like AI will emerge and advance as they always do, usually with unplanned, unanticipated, and even unimagined consequences. Take the advent of the smart phone and the internet—both are significant in their own right, affecting the way we live our lives and even how we fight our wars—but taken together, they have produced culture-changing phenomena like social media that many of us never saw coming. However, we adapted to those (for better or worse) as we always do, and I am not yet convinced that AI is so fundamentally different that it will have the economic and societal equivalent of an asteroid strike.

In the author's gloomy future, this mass displacement spares no country, developed or developing. It will be global, its impact so pervasive that the author wonders how all of those un- and underemployed workers will afford the goods that AI produces for them. This leads to an extended (and in my view, seemingly out of place) discussion about the advantages and disadvantages of Universal Basic Income, something the author clearly disdains but believes may be the only solution to the survival

Dr. Ronald Sanders is the Director, School of Public Affairs and a Clinical Professor at the University of Southern Florida. He has served as the Associate Director of National Intelligence for Human Capital, Director of Civilian Personnel for the Defense Department, and as Associate Director for Human Resource Policy at the Office of Personnel Management.

of the masses. . . in other words, those of us replaced by AI may need it to remain "happy" consumers of AI-derived products and services.

Plausible? Perhaps. Debatable? To be sure, but with that as a backdrop, the second and third parts of the book try to fulfill the much-anticipated promise of its title: "the future of leadership" in this brave new world. The good news here is that the author believes there is a future…she acknowledges that there will still be organizations (after all, who will find applications for AI?), and that those organizations will still need leaders, at least at the top of them. Indeed, according to the book, leaders are among the few organizational denizens that AI will not displace, though the author believes that those leaders will have machines rather than people reporting to them.

And how should those leaders respond to the challenge of AI? Much like part one, parts two and three of the book treat the reader to an exhaustive catalog of leadership prescriptions. . . lists and lists of dos and don'ts, the sum and substance of which may be summarized as "put people first."

Thus, as a general matter, the author argues that if we are to combat the tumultuous effects of AI, we must embrace humanism as a core leadership value. This is undoubtedly good advice in any context, and maybe this is the way ahead, the very one that those in the humanist school of leadership have been advocating since the Industrial Revolution.

But while the book offers AI-age leaders literally dozens of ways to do so—even as they replace millions of workers with this new technology!—it makes some implicit assumptions that may undermine its prescriptions for 21st century leaders.

For one, the book assumes that as those leaders confront AI (and a whole host of other challenges), they will do so at the helm of classic bureaucracies. Thus, although the author makes a few oblique references to a post-bureaucratic world, she implicitly defaults to hierarchy—and formal, chain-of-command authority—as the context for AI-age leaders and leadership, and this clearly influences the prescriptions that the book offers to them.

However, I believe that AI and all of its permutations will demand (and derive) different ways of organizing what we do, ones that are less hierarchical and more "netcentric" in nature. And in turn, those post-bureaucratic organizations will require a different paradigm for those who lead them.

That is certainly the case with organizations charged with achieving some public purpose, a distinction that the book does not address. Thus, 21st century elected officials, community leaders, career civil servants, and especially those in the military must lead in a world where no one of them has the formal authority to just say "make it so" and expect other countries, governments, institutions, and publics to obey. Rather, those leaders must be able to build and leverage networks—of other leaders, other organizations, other institutions, other governments—if they are to achieve unity of effort without reliance on unity of command. And AI will only exacerbate this reality.

Thus, in my view, this post-bureaucratic world—where AI is as much progeny as progenitor—requires a different leadership paradigm, one that is more complex than putting people first. What is that paradigm? I do not claim to have that answer (although I do have some ideas), but this is more than a practical or even a theoretical question. To me, it is existential, so our best minds—perhaps like those at NDU—best start thinking about it.

Notes

[1] For brevity's sake, and with apologies, I will refer to all of these technologies collectively as AI, even though I know better.

SUBSCRIPTIONS

Keep up to date with global and national security affairs, including sources, effects, and responses to international insecurity, global policy and development, nation-building and reconstruction, counterinsurgency, and lessons learned. To request your journal of complex operations, contact the *PRISM* editorial staff at <prism@ndu.edu>. Please include your preferred mailing address and desired number of copies in your message.


NATIONAL DEFENSE UNIVERSITY
PRISM
SCIRE QUOD SCIENDUM
INSS
INSTITUTE FOR NATIONAL
STRATEGIC STUDIES