SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Atlantic Council
STRATEGY PAPERS

A Candle in the Dark:

US National Security Strategy for Artificial Intelligence

Tate Nurkin and Stephen Rodriguez

Foreword by Secretary Ashton B. Carter

A Candle in the Dark:
US National Security Strategy for Artificial Intelligence

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

ISBN: 978-1-61977-077-5

Cover: Gift of the New York Gallery of the Fine Arts.
Digital image created by Oppenheimer Editions.

Title: Course of Empire: Destruction (4th in series)
Artist: Thomas Cole
Year: 1836
Medium: Oil on canvas
Size: 39¼ × 63½ inches

In the late 1820s, the young Thomas Cole, reknown for his Hudson River landscapes, conceived a cycle of paintings that would illustrate the rise and fall of a civilization. In the series "The Course of Empire", Cole presented a cyclical view of history in which a civilization appears, matures, and collapses. The motto he attached to the series was taken from Byron's popular poem: "First freedom, then glory; when that fails, wealth, vice, corruption." This fourth and most dramatic of the images in the cycle depicts the ruin of Cole's civilization. The city has fallen to a savage enemy. Instead of the statue of Minerva, goddess of wisdom, that kept watch over the third painting in the series, a headless colossal figure taken from the Louvre's Borghese Warrior witnesses the rapacious acts of the invading army. Unlike the other paintings, here Cole's signature is audaciously large and carved in slashing letters, almost like an act of vandalism, on the pedestal of the ruined statue at the right.

ATLANTIC COUNCIL STRATEGY PAPERS

EDITORIAL BOARD

TABLE OF CONTENTS

FOREWORD 02

INTRODUCTION 04

THE STRATEGIC CONTEXT 08

AI and Drivers of US National Security 08

Fractured Frameworks and Enhanced Competition 09

Liberalism, Nationalism, and Authoritarianism 14

The Information and Fourth Industrial Revolutions 16

Diffusion of the Power to Disrupt 17

Implications for US National Security and AI Strategy 17

Four Fusions 17

An Expanding Threat Spectrum and AI 21

A FRAMEWORK FOR UNDERSTANDING APPLIED AI 22

National Security Applications for AI 26

Intelligence and Decision-Making: Enhancing Processing and Cognition 26

Training and Simulation 28

Autonomous Platforms and Systems 30

Human Performance Enhancement 32

Logistics and Maintenance: Predictive Maintenance 34

Cognitive Sensing, Communications, and Electronic Werfare 34

Competition in and Exploitation of the Information Domain: Cyber Security and Deepfakes 36

Security, Surveillance, and Social Monitoring 39

GOALS AND ELEMENTS OF THE STRATEGY 42

Goals of the Strategy 43

Direct 44

Prioritization of AI Technology, Capabilities, and Effects 44

Integration of Prioritized Technologies 47

The Future 'Data Gap' and Facilitation of Data Sharing 49

Engage 51

Narrative Building 51

Process, Regulation, and Mindset 55

Govern 57

Ethics and Safety 58

Data Integrity and Privacy 59

Compete 61

Competitive Strategies 62

The Competition for Talent 65

Protect 68

Meeting the Theft and Acquisition Challenge 68

CONCLUSION 72

ABOUT THE AUTHORS 74

ACKNOWLEDGMENTS 76

FOREWORD

There is an intense and high-stakes competition being waged by the United States and its near-peer adversaries across a spectrum of emerging technologies, including Artificial Intelligence (AI). AI refers to technologies that use algorithms to learn from data, environment, and experience. The enhanced autonomy and rapid processing power it enables will effect significant changes in public and private sector operations, from data analysis to autonomous vehicles, weapons platforms, and virtual/augmented reality. AI is a paradigm shift—and as with any breakthrough development, innovation leaders will possess a significant advantage over their competitors.

Today, US adversaries continue to push the boundaries by developing innovative asymmetric advantages derived from these new technologies. A rising China is harnessing its state-owned enterprises (SOEs), multinational research centers, and defense industrial base, for unparalleled collaboration between its civilian and military spheres. Russia, less capable, nevertheless continues to engage in exploitative information campaigns that will only become more damaging with AI-enabled capabilities. At the same time, these adversaries employ a host of tactics meant to surreptitiously acquire US technology and intellectual property, shortcutting the research and development (R&D) process to enhance their competitive edge. The challenges posed by US adversaries will only increase in magnitude as AI becomes more pervasive in the commercial, public, and national security sectors.

In my prior role as US Secretary of Defense, I worked to better incorporate new AI technology into the US defense strategy, capabilities, and acquisition process. Despite the growing significance of AI to every facet of US national security, however, a coherent strategy that defines and articulates US policy has yet to materialize. The absence of a whole-of-government approach to the acquisition and exploitation of AI and its enabling capabilities is challenging, especially in light of growing competition with China and Russia. Ceding leadership at such a critical time of technological development poses a significant risk to the rules-based international system underpinned by the United States.

This Atlantic Council Strategy Paper, "A Candle in the Dark: US National Security Strategy for Artificial Intelligence," by Tate Nurkin and Stephen Rodriguez, effectively articulates the current technological landscape and offers a coherent strategic framework for the United States and its allies to harness AI's upside potential, while mitigating downside risks and defending against emerging threats. The authors are cleareyed about the challenges that will need to be overcome to make this strategy successful, including through improving cooperation between the United States and its allies, respectively between the private and public sectors.

The strategy provides recommendations along five lines of effort: **direct, engage, govern, compete, and protect. Direct** focuses on selecting, developing, and integrating prioritized areas of AI technology to support urgent US national security objectives, missions, and outcomes. Additionally, it calls for more open sharing of data across the US government, allied nations, and the private sector. **Engage** aims to better optimize the US innovation system by leveraging the high-tech community in the United States—and beyond—for national security. This goal requires the development of an effective strategic narrative to incentivize participation among the numerous relevant stakeholders. **Govern** promotes cooperation and collaboration with allies and multilateral institutions to establish and define standards and norms for AI safety and ethics. Stronger partnerships enhance the understanding of the risks associated with the use of biased or incomplete data, as well as the malicious corruption of data. **Compete** designates a means of more effectively contending in the AI and broader military-technological competition with China. To sustain the US advantage in AI development, we must leverage America's vast alliance networks. **Protect** describes proactive and focused measures to protect high-value US technology from acquisition by adversaries. China's aggressive technology acquisition program demands action to insulate the US innovation community from either illicit or licit technology transfers.

AI and its enabling technologies are at the center of the developing power competition between the United States and China. Establishing and sustaining US leadership in AI is critical for defending the United States and its allies, as well as maintaining the liberal values and norms on which the wider international geopolitical system is based. To compete in an increasingly technologically dominated global society, the United States requires a holistic artificial intelligence strategy that leverages its unique strengths. This Strategy Paper provides an excellent path to accomplish this goal and should be required reading for anyone concerned about America's technological competitiveness.

Ash Carter

Dr. Ashton B. Carter
Former US Secretary of Defense

ARSENY TOGULEV/UNSPLASH

INTRODUCTION

In 1996, astrophysicist and noted author Carl Sagan wrote a now-famous book titled, *The Demon-Haunted World: Science as a Candle in the Dark.* As he tried to help the reader understand the scientific method and discern between science and pseudoscience, he exclaimed, "There are wonders enough out there without our inventing any."[1] He could have been talking about artificial intelligence (AI).

The world is only at the start of the fourth industrial revolution (4IR) and the waves of digitization it will produce, but the transformative effects are already being felt. The combination of 4IR technologies has already digitized the media and telecom industries; now it is in the process of digitizing industry more broadly.[2] Many predict that the digitization of "society itself" will follow in coming years and potentially so, too, the integration of human and machine intelligence to the benefit of both.[3]

AI is at the core of this revolution in both the public and private sectors. Development and creative use of AI technologies may enable access to new horizons previously only contemplated by science fiction.

The implications of the development of these technologies for US national security are complicated and layered. For advanced militaries around the world, the demand for AI-enabled capabilities is surging to deliver improved decision-making, readiness, and operational effectiveness. AI technologies also will enable novel capabilities—drone swarms and fully autonomous platforms and systems—that have the potential to upset both carefully crafted and maintained military balances and stabilize imbalances in geopolitical and military domain area competitions.

But the impact of AI on US national security goes well beyond new capabilities, as strategically significant as these changes are. Savvy employment of AI technologies poses threats to the political and societal stability of the United States and allied nations; the dislocation of many service-sector jobs is chief among them.

Furthermore, AI use in support of authoritarian control in China—and by other actors—and the likelihood that AI-driven instruments of control diffuse to more state and non-state actors pose a fundamental challenge to US values, the norms and principles on which the international system operates, and, as a result, to US national security. Can US security, stability, and prosperity be preserved, much less advanced, in a world in which tools of social control are widely proliferated?

Probably. But this world—which is an extrapolation of empirically observable trends, not an invention of pseudo social science—will create different competitions and mandate new approaches to US national security

This context for US national security requires a whole-of-government approach, working with allies, to ensure continued US leadership, not only in researching AI technology, but also in devising creative AI applications and developing standards and norms for AI ethics and safety. Specifically, this approach should be built around five linked concepts:

- **Direct:** The US government (USG) needs to determine and align priority areas of AI technology capability development to meet the most urgent and affecting challenges and capitalize on the biggest opportunities for US national security. Priority should also be given to identifying gaps in the AI knowledge base within the United States as well as its allies and competitors.

- **Engage:** The US high-tech industry is a critical but underleveraged asset in ensuring US national security. Designing narratives and reforming government business

Defining AI: Technologies, Capabilities, and Applications

AI does not have a clear definition, though the term is typically used to describe machines capable of learning from their environment to achieve an objective without explicitly being programmed to do so. AI is not a specific technology, and there are a range of different types of AI techniques, each of which can be applied in different and creative ways by the individual or organization deploying them. This paper is largely focused on types of AI techniques listed below. It also seeks to differentiate between AI techniques and the technological innovation behind these techniques and the capabilities they enable as well as the specific applications of AI-enabled capabilities in support of mission sets or defense and security objectives.

AI Technologies of particular interest to this paper:

- machine learning
- deep learning/neural networks
- computer vision
- facial and voice recognition
- particle swarm optimization
- adversarial examples
- natural language processing

practices to garner more widespread high-tech and applied research buy-in to prioritizing support to US defense and security communities could unleash a powerful enabler of US security and stability. Engagement with the American public on the nature and implications of the opportunities and risks related to AI development and AI-enabled capabilities is also a component of the engage concept.

- **Govern:** The United States should lead the discussion of AI ethics and safety, especially in the context of AI use for security, defense, and surveillance purposes. Devising prioritized recommendations at local, state, and national levels and internationally will require more research on AI safety and ethics to help parse the ethical complexities of AI in a way that avoids stifling salutary development of AI technologies, but nonetheless places material safeguards against its most deleterious and menacing applications.
- **Compete:** All decisions and actions taken to further the development of AI for US national security must be viewed through the context of geopolitical competition. The most serious adversary in this competition is China, but policy makers should not ignore Russia. Development of AI and other emerging technology areas including the fifth-generation mobile network (5G), quantum computing, next-generation semiconductors, and robotics is an increasingly important and fractious component of this competition. Without collaboration with allies and partners, the United States risks falling behind in this decisive competition of the twenty-first century.
- **Protect:** Efforts to protect strategic AI technology developed within the United States cut across each of the other four concepts and should incorporate a combination of crafting of narratives for domestic and international consumption as well as calibrated regulations and incentives for US private capital to support the technology areas prioritized as part of the direct component of the strategy.

Unfortunately, to date, the United States has lagged behind much of the advanced world in the development of a whole-of-government AI strategy. Other advanced nations boast both general and national security-oriented AI strategies.

China announced its Next Generation Artificial Intelligence Development Plan in July 2017 and has executed aggressively against the ambitious objective of becoming the global leader in AI by 2030, including in AI applications for national and state (read “regime”) security.[4] Russian President Vladimir Putin ordered that Russia’s national AI strategy—which includes a prominent role for the Ministry of Defense—be completed in June 2019. Russia’s strategy will be the seventeenth published national AI strategy document to go along with two additional regional AI strategy policies (the European Union and Nordic-Baltic states). The nature of these strategies varies considerably, of course. Some constitute high-level aspirational guidance documents while others are more comprehensive and include fully funded policy commitments.[5]

The United States has yet to release a formal whole-of-government AI strategy, though it has not been entirely silent on the issue of AI development, in particular for national security. In May 2019, US Senators Rob Portman (R-OH), Martin Heinrich (D-NM), and Brian Schatz (D-HI) introduced the Artificial Intelligence Initiative Act, which would make $2.2 billion of funding available to several government agencies over five years for federal research and development in support of the creation of a national AI strategy.[6]

The announcement follows a flurry of AI strategy-focused activity in February 2019. On February 11, the White House released the Executive Order on Maintaining American Leadership in Artificial Intelligence. The document articulated principles, objectives, and policy priorities for the United States to guide AI development efforts in support of economic, development, societal, and national security objectives.[7] The executive order is a useful, but vague, document most notable for injecting a sense of urgency into the discussion of US approaches to AI development and for articulating principles around which future strategies should be built.

The following day, the US Department of Defense (DoD) released its own Artificial Intelligence Development Strategy, which detailed five high-level objectives for DoD investment in AI technologies and applications:[8]

- delivering AI-enabled capabilities that address key missions
- scaling AI's impact across DoD through a common foundation that enables decentralized development and experimentation
- cultivating a leading AI workforce
- engaging with commercial, academic, and international allies and partners
- leading in military ethics and AI safety[9]

As did the executive order, DoD's strategy shone a light on the mounting interest in AI-enabled capabilities across the US government. It delivered a "30,000 feet" set of guiding principles to bound and guide key future initiatives, such as the Defense Advanced Research Project Agency's (DARPA) $2 billion AI Next program[10] and the Joint Artificial Intelligence Center (JAIC), both of which seek to sustain US advantage in this critical technology area.

Together, individual measures across DoD and the government more broadly signal a United States government that recognizes but is still trying to diagnose the full suite of issues around which an AI strategy for national security should be built. To date, US actions have been sporadic, decentralized, and uncoordinated—especially compared with China's comprehensive, ambitious plan. Now is the time for parallel efforts to 1) consolidate perspective, knowledge, and capability across the USG and 2) increase communication, cooperation, and trust with the high-tech industry.

MAARTEN VAN DEN HEUVEL/UNSPLASH

THE STRATEGIC CONTEXT

AI AND DRIVERS OF US NATIONAL SECURITY

American AI development will take place within a complex, competitive, and challenging strategic geopolitical and security context that will both shape and be shaped by how the United States, China, and other actors, develop, diffuse, and deploy various AI technologies and the capabilities they enable.

The United Kingdom Ministry of Defence's 2018 *Global Strategic Trends Report* provides a revealing assessment of the intensity and uncertainty associated with the intersection between the global strategic context and AI.

The report includes a chart that places sixteen forces affecting the future security environment (see text box) along two axes: an X-axis of *uncertainty* and a Y-axis of *impact.* The driver "Harnessing Artificial Intelligence" was depicted as:

- being the most impactful;
- having the second most uncertainty about how it will develop (behind only erosion of state sovereignty); and
- generating the second most variance of assessment of the experts and analysts that contributed to the report.[11]

Put another way, AI is expected to have a powerful impact on the future of geopolitics, defense, and security, but the exact nature of this effect will depend on decisions and actions influenced by the intersections between other trends, drivers, and uncertainties. Four forces are particularly relevant to the intersection between the capacity of state and non-state actors to harness AI, with an impact on US national security.

16 Strategic Drivers from the UK's Global Strategic Trends Report:

1. Harnessing artificial intelligence
2. An expanding competitive space
3. Increasing proliferation of weapons of mass effect
4. Erosion of state sovereignty
5. Adaptation of the rules-based international system
6. An expanded and unregulated information space
7. Rising inequality, reducing social cohesion, and fragmented societies
8. Understanding human enhancement
9. Increasing competition in the global commons
10. Increasing disruption and cost of climate change
11. Increasing demand and competition for resources
12. Greater automation and an increasingly diverse workforce
13. Managing technological change
14. The challenge of affordability
15. Increasing threat from crime and extremism
16. Managing demographic change

Fractured Frameworks and Enhanced Competition

Geopolitical frameworks, alignments, and norms that have sustained and generally governed relations among states over the last seventy years are eroding and being challenged in stark ways. Among the results: increased competition across the international system by actors seeking to gain advantage in revising the rules and parameters of a world in transition.

China and Russia both have consistently raised this theme of a changing geopolitical environment in official documents since at least 2013. China's 2015 *Science of Military Strategy*—an authoritative book published by the Academy of Military Sciences of the People's Liberation Army (PLA)—describes the move from an "unprecedentedly unipolar" world to a new twenty-first century "international balance that is characterized by multi-polarity and co-governance."[12] The United States may still be the world's only superpower, but China is a central player in this rebalanced world of diminishing US power and influence. China has the opportunity to use globalization and the informatization of society to propel itself forward economically, socially, and technologically.[13] Russia's 2013 Foreign Policy Concept refers to "the deep-seated transformation of the geopolitical landscape" to a "polycentric or multipolar world."[14] For its part, the United States now understands the competitive dynamics that dominate the global defense, security, and geopolitical environment. This acknowledgement is codified in the 2018 United States *National Defense Strategy,* which identifies competition with Russia and especially China as the most pressing national security and defense challenges and priorities.[15]

US-China Geostrategic Competition

The US-China geostrategic competition has evolved as the postures of both states have shifted over the past two to three decades. The United States has moved from an externally focused leader of the international system to a country distracted by political polarization and dysfunction and, among some constituencies, tiring of shouldering the burden of global leadership. China's transition has proceeded along a different trajectory. It has moved at an accelerated pace in particularly the 2010s from a country largely constrained and driven by its vulnerability to US and allied economic, geopolitical, and military power to one confident in its own power. As a result, China has become more ambitious in its objectives to challenge and alter the rules of the US-led, rules-based system.

The US foreign policy, security, and defense establishment sees a world in which existing geopolitical frameworks are generally beneficial and benevolent—in need of refinement and adjustment, but ultimately salvageable. China sees a window of opportunity to capitalize on global geopolitical uncertainty and transition not to refine the rules of the geopolitical and economic order, but rather to rewrite them in a way that will enable China to:

- optimize its economic growth and geopolitical influence;
- export its techno-authoritarian model; and
- ensure the long-term security and sustainability of the Chinese Communist Party (CCP) regime.

This tension is the crux of the competition.

The dynamics result from escalating US-China tensions manifest in provocative ways that reflect a high-stakes and expanding geostrategic competition: close calls between military platforms in air and sea, freedom-of-navigation operations, the trade war, growing competition in global defense export markets and infrastructure development, aggressive technology theft and protection efforts, and a rapidly increasing technology competition, among many others.

Professor Xiang Songzuo, a former chief economist of China Agriculture Bank, captured the concept of a broad and systems-based competition in a December 2018 speech at Renmin University School of Finance. Speaking of the trade war, Xiang noted that "it is no longer a trade war, but a serious conflict between the Chinese and American systems of values. The China-US relationship is at a crossroads and so far there has been no solution found to resolve their differences."[16]

Technology Competition and China's AI Development for National Security

Technology development and acquisition—especially in AI—is a critical part of this expanding competition. For China's leaders, gaining advantage in AI, as well as enabling technologies such as semiconductors, 5G networks, robotics, quantum computing, and neuroscience, is central to economic transformation and geopolitical influence, as well as the ability to manage disruptive internal social, demographic, and political forces.

These and other technologies are crucial to a military modernization program that has seen sustained and consistent forward momentum in the development of advanced antiaccess/area-denial (A2/AD) capabilities, and the progress is already rearranging the military balances and stabilizing imbalances that have helped sustain security in the Indo-Pacific for the last two decades. China's recent focus on indigenous aircraft carrier, destroyer, strategic lift, and aerial refueling assets as well as overseas basing has extended China's global reach and, as a result, influence.

AI will further China's A2/AD and power-projection efforts, but the most relevant and, over the next ten to fifteen years, most impactful intersection between AI and PLA modernization is the Chinese military transition from informatized to "intelligentized" or cognitive warfare.[17] Over the last decade or so, the PLA has been optimized to operate in the highly "informatized" conditions of modern warfare that emphasize connectivity, networked forces, increased access to information, and ease and pace of communications. These capability trends are still relevant, but are being augmented—and eventually will be superseded—by AI-enabled cognitive and autonomous capabilities. The intelligentization of conflict—both traditional kinetic military operations and those in the information domain—presents China with an opportunity to shift the nature of its military competition with the United States from a position of perpetually needing to catch up to the US defense industrial base to being able to establish, maintain, and solidify advantage in the race to the commanding heights of cognitive warfare.

China is demonstrating innovation competency—and in some areas possibly even world leadership—in AI-enabled military and security applications that will be critical to the future of conflict. For example, much has been made of China Electronics and Technology Group Corporation's (CETC) June 2017 successful test of a swarm of 119 drones, then the world's largest test of a drone swarm for military purposes. A similarly important development was the May 2018 test by Yungzhou Technologies of an unmanned surface vehicle swarm of fifty-six ships that formed the outline of the *Liaoning*—China's first aircraft carrier—and the characters for "military" and "people" that symbolize military-civilian fusion,[18] less than subtle signals of the intended military application of this capability.

China's AI development for both military and civil purposes is buttressed by an innovation system that leverages its unique political, social, economic, and cultural characteristics. This system rests first and foremost on a centralized political and economic apparatus—long thought to be the source of inefficiencies in China's national development—that can marshal and, more to the point, direct the resources of its science and technology and commercial high-tech community in a way that is not easily replicated in the United States. The central direction and control have implications for collaboration between civilian and military enterprises, for data collection, storage, and use, and for the acquisition and transfer of technologies from the civilian sector to the military through military-civilian fusion.

Direction has taken the form of China's Next (New) Generation Artificial Intelligence Development Plan. Released in July 2017, the three-phased plan articulates a comprehensive pathway for China to become the global leader in AI by 2030—a relatively quick time frame for a country that has traditionally targeted more notional dates at or near the middle of the century for science- and technology-related leadership. The plan establishes actual objectives and priorities for AI research and development, technology focus areas, economic applications, size of the national AI industry, governance approaches, and talent development and training, an especially active area of US-China competition.

The plan is considered the most detailed and ambitious of the national intelligence plans published to date[19] and clearly catalyzed investment and increased competition in China's high-tech sector, which was already considered a highly competitive industry. It also appears to have stimulated Chinese industry to invest in and incorporate AI into business operations in a material way. A Boston Consulting Group report assesses that 85 percent of Chinese companies are "players" in the field of AI, meaning that these companies are making progress in incorporating AI into business processes.[20]

China's AI development has been supported by widespread theft and creative use of licit means to acquire US and Western technologies to include establishing innovation centers in China in conjunction with leading American high-tech firms such as Amazon, Microsoft, and Google. [21] So pervasive is concern about China's technology theft and acquisition that in July 2018, FBI Director Christopher Wray asserted that "China, from a counterintelligence perspective, in many ways represents the broadest, most challenging, most significant threat we face as a country."[22]

Ultimately, as the US-China geostrategic competition plays out over the next decade and beyond, AI development for national security purposes will play an ever-more important role. Both states will work to leverage their relative strengths, mitigate their vulnerabilities, and, critically, shape a global AI research, development, and deployment environment that reinforces competitive asymmetries and advantages.

Category	Current US Advantages	Current Chinese Advantages
Research, development, and applications	AI science and core concepts	Ability to take core concepts and create innovative AI applications, especially in the commercial information and communications technology (ICT) industry
Enabling technologies	Semiconductors	5G networks and quantum computing[23]
Domestic high-tech industry	Global leading high-tech industry, though there have been challenges in fully optimizing this industry for national security purposes	Ability to leverage commercial high-tech innovation and technology/knowledge acquisition for military purposes through government direction and pressure and mechanism of military-civilian fusion

Table 1: Simplified high-level depiction of relative advantages of the AI-related innovation systems of the United States and China according to the authors.

SOURCE: TATE NURKIN AND STEPHEN RODRIGUEZ

Russia

The dimensions and stakes of the US-Russia competition are different. China and the United States are competing to make and sustain the rules governing future international relations. It is a contest of strong—though far from invulnerable—polities and societies.

Russia is by most national measures a country experiencing extended decline. To be sure, it has reasserted itself on the global stage in a significant way over the last decade through a series of provocative actions. Imposing its will on Georgia in 2008, seizing Crimea in 2014, and fomenting instability in Syria in present day; these actions are reflective not of enduring or foundational national strength, but rather of a country suffering from a number of domestic economic, demographic, social, and industrial-base challenges.

But even a declining Russia poses a persistent challenge to the United States and its allies as Moscow takes more risks to enhance its security, remain competitive, and to further the transition of the international system away from Western-led frameworks. Moreover, Russia has demonstrated an impressive aptitude at using the resources and asymmetric tools it does possess in creative and unexpected ways that ultimately maximize their operational and strategic impact. Russia's ability to implement disinformation and influence campaigns that successfully amplified social and political discord and undermined elections in the United States and Europe is well-documented, as is its use of influence operations in conjunction with "little green men."[24]

AI-enabled cyber and information operations capabilities offer Russia a formidable tool in its asymmetric weapons and hybrid warfare toolbox that can serve as a force multiplier in Russia's efforts to weaken the United States and its allies, especially in Europe. In addition, Russia has invested in autonomous platforms and systems, such as the Uran-9 autonomous unmanned ground combat system. The system had a notoriously failed deployment to Syria, but Russian development of autonomous unmanned ground vehicles, including unmanned ground combat vehicles, continues.[25] Similarly, President Putin announced on February 20, 2019, that Russia will launch the first Poseidon autonomous unmanned underwater vehicle. The Poseidon is a nuclear-powered, nuclear-armed unmanned autonomous undersea vehicle—essentially a long-range nuclear-armed torpedo—precisely the sort of provocative, disruptive, and potentially destabilizing capability Russia in decline has tended to favor.

Russia's current (unclassified) investment levels in AI are significantly behind the United States and China, at approximately 700 million rubles ($11 million).[26] The Russian market for AI technology will remain orders of magnitude smaller than that of the United States and China, even if the significant forecasted growth to 28 billion rubles (approximately $440 million) by 2020 is realized.[27]

Achieving success in AI for military applications would require Russia's military to leverage its small but growing domestic AI industry. In March 2018, Russian Defense Minister Sergei Shoigu encouraged Russia's domestic civilian AI technology industry to join forces with the armed forces to "counter possible threats in the field of technological and economic security of Russia."[28]

In July 2018, the Russian Ministry of Defense (MoD) and Ministry of Education and Science (MES) released a joint ten-point plan for Russia's whole-of-government approach to developing AI for military purposes that emphasized:[29]

- **creating mechanisms for consolidation and collaboration** among academic, government, and defense AI development efforts including forming an AI and Big Data consortium, building an AI lab at the Era science and technology research and development center, establishing a National Center for AI, and holding an annual AI conference to facilitate collaboration between government and academia;
- **skills and talent development** through gaining automation expertise and developing a state system for AI training and education;
- **socializing the opportunities and challenges of AI for defense purposes** by testing AI-focused scenarios that explore the impacts of AI models on military tactics and operations and discussing AI capabilities and proposals at Russia-hosted military forums such as the Army 2018 Exhibition; and
- **focused collection** on global AI developments and trends to better understand the research and development approach and priorities of other countries.

Russia has worked to further refine and develop these concepts and principles over the last year or so with the objective of releasing an overall AI strategy in 2019. In October 2019, after several delays, Russia released its national AI strategy, which actually makes no explicit mention of AI development for national security or defense purposes. The strongly state-led strategy stresses talent recruitment and retention as well as education and on access to public data to improve AI research and development by the Russian government and government-sponsored organizations.[30]

Liberalism, Nationalism, and Authoritarianism

U.S. competition with China and Russia coincides with a second driver of the emerging geopolitical and security context influencing the future of AI technology development: conflict between liberalism and authoritarianism. The values and principles of the former (individual liberty, social trust, democracy, rules-based systems, and institutional checks and balances on government exercises of authority) clash with those of the latter (an absence of these things—or at the very least diminution of them—in favor of reinforcement of the authority of the state, regime survival, and social and political control.)

As Robert Kagan explained in a March 2019 *Washington Post* article, the erosion of the geopolitical frameworks discussed above as well as the manifold social and political pressures of the modern world have created an opening for authoritarianism and authoritarian regimes to call into question the legitimacy and potency of specific liberal democratic governments, including more fundamentally, the liberal democratic ideal.[31]

The narrative has resonance across authoritarian regimes and within states and societies that may chafe at the perceived disconnect between the externally focused remonstrations of liberal democracies and the inability of these governments to effectively deal with social and economic equality issues within their own borders. It also has gained traction in socially and economically displaced communities and nationalist groups in liberal democracies possessed by a growing list of complaints about immigration, globalization, elites, wealth disparities, corruption, and a general perceived inability of central sovereigns to respond to modern challenges and control all of the territory, populations, institutions, and resources within their prescribed borders.

Varying forms and degrees of authoritarianism offer an alternative to liberalism, one that stresses an ability to meet challenges of the modern age more nimbly and efficiently than frequently messy and inefficient democracies, at least in the short term. Over time, of course, the commitment to process, institutional strength, and deliberation provide resilience. But in the age of twenty-four-hour news cycles and social media saturation, the immediate and simple solutions and messages of more efficient control and prioritizing of results over process have an appeal that can be difficult to counter.

AI and other emerging technologies and social media platforms are a central part of this competition between authoritarianism and, to date, mostly passive liberal democracies. As Kagan noted, "new and hitherto unimaginable tools of social control and disruption . . . are shoring up authoritarian rule at home, spreading it abroad, and reaching into the very heart of liberal societies to undermine them from within."[32] Or, as Richard Fontaine and Kara Frederick laid out in an essay entitled "The Autocrat's New Tool Kit," these AI-enabled tools will "allow strongmen and police states to bolster their internal grip, undermine basic rights, and spread illiberal practices beyond their own borders."[33] The main AI technologies being applied for internal security are facial and voice recognition, as well as machine learning applications that can help separate loyal citizens from potentially disloyal ones, target minority ethnic groups, and identify and deploy tailored influence and persuasion messages.

China and Russia are the most active in developing and deploying these capabilities. Moscow already has more than five thousand cameras installed with facial-recognition technology, which the Russian government can reportedly use to match "faces of interest" to photos from passport databases, police files, and social media feeds.[34] In May 2019, the Russian government announced that it would apply a new facial recognition system to link all 160,000 surveillance cameras across Moscow.[35] China's use of facial recognition software and machine learning to surveil its population is well-documented over much of 2018 and 2019, including in support of monitoring over five hundred thousand Uighur Muslims in Xinjiang province and instituting "social credit scores."

The Information and Fourth Industrial Revolutions

The pervasiveness of social media use and 4IR-driven digitization of industries serve as a powerful driver of escalating geopolitical competition, as well as the development of national security-focused AI technologies.

And the 4IR is *only at its beginning.* State, regional, and global economies have yet to experience or even fully comprehend the transformative potential of the combined and individual effect of 4IR technologies (see text box).

So far, though, at least three additional key implications relevant to efforts to build a US AI development strategy are already visible.

First, the adoption of 4IR technologies will create "winners" and "losers"—those that benefit from technological innovation and the connectivity and efficiency it creates and those who either are or *are made to feel as if they are* left behind by a hurtling and dislocating modernity. Pervasive perceptions of perpetually threatened communities will amplify the social fissures that can be exploited through the savvy use of the information domain and social media and further call into question the legitimacy of liberal democratic values and governance models. In short, innovation in AI technologies will enable new means of weaponizing information and the networks through which it is passed with potentially powerful strategic and operational effects for US political stability and institutional efficacy.

Second, AI and 4IR technologies are shaping the future of military capabilities and potentially changing the nature of conflict and warfare altogether. Over time, they could remove important human components to combat and introduce new norms, operational concepts, and domain areas for competition.

Deployment of new technology-enabled capabilities will require development of new operational concepts in order to optimize their strategic, operational, and tactical utility. It will also mandate a reassessment of commonly held assumptions about escalation, deterrence, dissuasion, technology diffusion, and military advantage in a hybrid world in which the physical and digital are merged. Multilateral discussion, much less agreement, on new protocols is likely to lag behind the development of the capabilities themselves. This disconnect could enhance the possibility for unintentional escalation, miscalculation, and even preemption in the fast moving and complex strategic and operational environment of future crises and conflicts.

Third, AI's national security implications are magnified by its intersection with other 4IR technologies. Quantum computing, cloud computing robotics, neurotechnologies and biotechnologies, smart materials, and sensors all offer methods for either improving AI efficiency or generating new AI-enabled security-focused applications.

Technologies Associated with the 4IR

- AI
- Internet of Things
- cloud computing
- quantum computing
- big data analytics
- robotics
- blockchain
- smart materials
- additive manufacturing and multi-dimensional printing
- biotechnologies
- neurotechnologies
- smart sensors
- virtual and augmented reality
- energy capture and storage
- space technologies

Diffusion of the Power to Disrupt

More actors are able to affect strategic and operational environments—from global and regional powers and transnational networks to galvanizing personalities and ideologically imbued and technologically savvy individuals. These actors are empowered by their ability to exploit the information domain, but also because they are in command of or have access to more and more sophisticated capabilities. This trend is in large part due to the diffusion of a broader range of emerging technologies including AI.

This diffusion is happening simultaneously through licit and surreptitious means, ranging from mergers and acquisitions and joint ventures to cybertheft, traditional espionage, and the use of nontraditional collectors.

Defense export market dynamics provide a particularly relevant licit pathway for diffusion. Since approximately 2010, emerging markets in Asia, the Arabian Gulf, Eastern Europe, and some parts of Latin America have sought to use growing leverage vis-à-vis defense contractors to build or enhance their respective domestic defense-industrial bases. Sales to some of the biggest export markets in the world now come with expectations of offsets in the form of technology transfer, joint development, long-term product line support, and technical training. Some companies—especially those in the United States—are constrained by shareholders, legal frameworks, and business savvy from exporting their most sensitive technologies. Other companies and state-controlled enterprises are far less reticent to give away the "crown jewels," especially in a savagely competitive defense market.

China's exports of unmanned aerial vehicles adroitly exploit these dynamics—as well as US abdication from the armed unmanned systems market. Chinese deals with Pakistan and Saudi Arabia both included joint development provisions. Passing on the technological secrets of CH-4 and Wing Loong drones is a small price to pay for China to close deals that solidify commercial and geopolitical relationships in strategically important countries.[36]

The dual-use nature of many 4IR technologies also facilitates their diffusion to state and non-state actors. Many of the technologies driving the future of military capabilities are also being developed by the high-tech industry, applied research institutes, and industries such as automotive and commercial aerospace. Acquisition eases diffusion through these nondefense, and therefore less restricted industries. Indeed, some emerging technologies—like drones, software, encryption tools, virtual and augmented reality, and additive manufacturing—are actually commercially available as well.

IMPLICATIONS FOR US NATIONAL SECURITY AND AI STRATEGY

Four Fusions

The interplay of these drivers has created an environment characterized by the deepening of four fusions of previously mostly separate concepts or conditions. Both individually and collectively, these fusions have immense implications for how the United States may leverage AI to maintain US security, stability, and prosperity and how competitors and non-state actors will use AI and other 4IR technologies to counter these efforts and undermine US security.

An Unsettled World: The Fusion of States of Peace and Conflict

Competition and technology development and diffusion have created an unsettled world, in which the states of peace and conflict are blurred.

Russia was early to recognize the fusion of peace and conflict and has built both strategic and operational doctrines around it. General Valery Gerasimov, chief of staff of the Armed Forces of the Russian Federation, has repeatedly articulated the importance of using “asymmetric” information operations to achieve objectives without resorting to kinetic conflict or—in conjunction with “classical” military capabilities—to undermine the capacity of targeted adversaries to resist traditional military advances, such as in Crimea.[37] Most recently, in March 2019, General Gerasimov gave a speech in which he cited operations in Syria as an example of the success of this hybrid-warfare approach to conflict.[38]

A better example of the doctrine and how the merging of states of peace and conflict manifests itself is the Russian interference in the 2016 US presidential election. This was a bold, provocative action taken to subvert not military capability, but societal cohesion and foundational democratic processes, principles, institutions, and values. Interventions and manipulations were designed to strike at the heart of the American society and polity in a way that was unlikely to be achievable in the modern strategic context via traditional military means without risking a potentially catastrophic escalation.

Ironically, only a few days after General Gerasimov’s March speech, the cybersecurity firm Recorded Future released a report raising awareness for the subthreshold threats emanating from the information domain and social media. The main takeaway: Western governments and—perhaps more importantly in a dual-use world—social media companies are unprepared to counter offensive information operations from Russia and China.[39]

Risk-taking and boundary pushing, figuratively and literally, from some actors are more prevalent as a result of the perception of a perpetual state of hypercompetitive conflict, even if that conflict stops short of being a shooting, rather than a trade, war. And the risks of “rule breaking” are increasingly tolerable in many instances because the capabilities employed tend to muddy the waters of detection, attribution, and intent in ways that make deterrence, dissuasion, and effective signaling much more difficult. This has placed considerable pressure on international law structures, which have not adapted to this new reality. This tactic is evident in the use of little green men, patriotic hackers, and civilian maritime militia. AI is poised to unleash new and enhanced means of operating in this unsettled world, especially through AI-infused cyberattacks and through greatly enhancing the ability of actors to target disinformation campaigns or more efficient election manipulation efforts. These particular attack vectors only scratch the surface of the threats that AI could unleash.

A Hybrid World: The Fusion of the Physical and Digital

Some of these new capabilities are generated by the fact that the boundaries between the physical and digital have eroded as more physical items become connected to the Internet and to each other. Recent estimates are that approximately thirty billion devices will be connected by 2020.[40] AI, virtual and augmented reality, biotechnologies and neurotechnologies, robotics, and cloud computing all conspire to strengthen the seamlessness of interactions and activities taking place across the physical and digital worlds.

Connectivity brings efficiency and convenience. It also brings vulnerability; the promise of the fusion of the digital and physical world is balanced by potential peril for US national security, particularly as AI-enabled smart bots make it difficult to distinguish between interactions with humans from those with bots deployed to manipulate, influence, and outrage.[41]

Perhaps more alarmingly, the fusion between physical and digital worlds is also taking place outside of the information domain. Military and security communities are experimenting with ways to incorporate novel 4IR technologies and AI applications that link the humans and machines to improve decision-making, physical endurance, and performance.

A Manipulated World: The Fusion of Reality and Perception

The strategic context is also one marked by the fusing of reality and perceptions in ways that obliterate assumptions about the nature of facts, truth, and verisimilitude. The modern, competitive, narrative-centric, and, mainly, *manipulated* world resembles Nietzsche's perspectivist retort to empiricist claims of the primacy of facts: "no, facts is precisely what there is not, only interpretations."[42] Or, more simply put, Simon and Garfunkel's perception that "a man hears what he wants to hear and disregards the rest."[43]

Even in cases where there is established scientific or empirical evidence—for instance, Russian meddling in elections in the United States and across Europe—"alternative facts" are invented or distorted and accepted by millions at all gradients of the political spectrums as comforting support for an otherwise easily falsifiable contrary interpretation. Unfortunately, although some had predicted that the Internet would create a world of openness and transparency, AI instead threatens to deepen the segregation of the web into echo chambers predominated by homogenous, and alarmingly extreme, views.

Influence operations using deepfakes, which are manipulated video or other digital content produced using AI, will exploit the degradation of the truth to create and intensify divisive polarities and also offer sufficient justification for the instinct to retrench, to double down on interpretation and perspective in the face of established—but still debated—facts. In addition, the surprises and national security challenges of the manipulated world also extend to the operational environment. As the volume and velocity of information becoming available to intelligence analysts and decision makers increases, so does the vulnerability to AI-enabled "spoofing" attacks.[44] Whether AI is more helpful in sorting through the metaphorical haystack, or throwing more chaff on it, will prove a critical question for intelligence agencies worldwide.

A Dual-use World: The Fusion of Security and Commercial Demand and Interests

The intersection of the 4IR and geopolitical competition is merging technology demands of national security communities and the high-tech industry and other commercial entities.

Interindustry demand for autonomous systems, connectivity, bandwidth, network security, new types of energy and propulsion, space-based communications, new materials, and new manufacturing techniques has pushed the production of militarily relevant technologies outside of solely the traditional defense industry. The high-tech, automotive, and commercial aerospace industries, among others, have equally as pronounced interests in these technology and capability areas and are investing in capital and expertise in their development. The dual-use nature of these technologies, then, has expanded the parameters of what constitutes the defense industry at a national and international level. Governments and national-security communities are facing pressure to respond to these new dimensions with new maps—new processes for engagement, integration of civilian technologies for military purposes, and acquisition. Some countries have moved faster than others, and the disconnect between the US high-tech and national security communities constitutes a strategic vulnerability.

Geopolitical competition and the value-based struggle between liberalism and authoritarianism adds a different dimension to the complexities of the dual-use world. Private companies and academia must now consider positive control of strategic dual-use know-how and technologies as much as revenue expansion and international collaboration when doing business abroad; this is especially true in China or with companies that also sit in Chinese companies' supply chains. AI is at the top of the list of the in-demand technologies due to its perceived transformative potential and broad applicability to commercial, civilian government, and security activities. It is certainly a priority target for China's aggressive and centrally directed technology acquisition effort and military-civilian fusion mechanism through which commercial technologies are transferred and adapted for military and security purposes.

The proliferation of emerging dual use and commercial technologies is difficult to track, which also complicates the task of determining who has what technologies, how these technologies might be used, and, as a result, the nature of military-technological balances. Already, relatively simple and otherwise nonthreatening commercially available technologies—electromagnetic jammers, unmanned systems, cyber capabilities and even laser pointers—are being used in novel ways to create risks for military and security operations as well as softer, civilian targets and national security concerns such as critical infrastructure.

An Expanding Threat Spectrum and AI

In this context, the United States faces an expanded and uncertain threat environment in which the origin, pace, nature, trajectory, and dimensions of challenges to US national security, stability, and prosperity will be difficult to determine, much less anticipate and deter. Threats and challenges to US and allied national security and global stability will likely be multidimensional, requiring coordinated military responses not just between DoD agencies and services, but also with other government agencies and, frequently, allies and partners. Going it alone is more likely to create more security challenges and geopolitical pressures.

These security challenges are unfolding at two levels.

First, development and diffusion of novel technologies, especially AI, are together creating the conditions in which the primacy of US military-technological overmatch is being contested, though not yet overturned. Adversaries and competitors are developing new capabilities to hold at-risk vulnerable command and control nodes in the highly networked and digitized US military. Expectations of continued US superiority in space, the information domain, and electromagnetic spectrum in particular should be reevaluated, not because loss of leadership is a foregone conclusion—far from it—but because vigilance and urgency are required to retain this leadership.

Advanced weapons systems such as those enabled by AI, unmanned systems, counterspace, directed energy, hypersonic, and electromagnetic weapons are a "game-changer and game-leveler," according to a *Jane's* report published by the US-China Economic and Security Review Commission in May 2018.[45] Moreover, continued "intelligentization" of warfare also offers competitors a means of shifting the nature of conflict toward AI-enabled capabilities and therefore of challenging US military superiority over time.

Second, and perhaps more unsettling, is the idea that US military-technological overmatch–even if it is maintained—may not be as relevant to ensuring US national security in the current and emerging geopolitical and security context. To be sure, the ability to deter traditional threats to the US homeland, global interests, assets, and allies is and will continue to be critical to concepts of US national security. However, in the competitive, dual-use technology-infused environment, state and non-state actors have more and more powerful means of threatening US security by destabilizing the US polity, society, economy, and infrastructure through exploitation of information technologies and crafty narratives.

Here is precisely where AI may have the most significant impact on US national security: by empowering more efficient means of manipulating the political, societal, and cultural environments, fissures, and tensions in the United States and its allies. Of course, the good news is that the United States retains global leadership in AI development and these capabilities offer equally the potential to detect and defeat these new threats and challenges as well.

JOÃO ROCHA/UNSPLASH

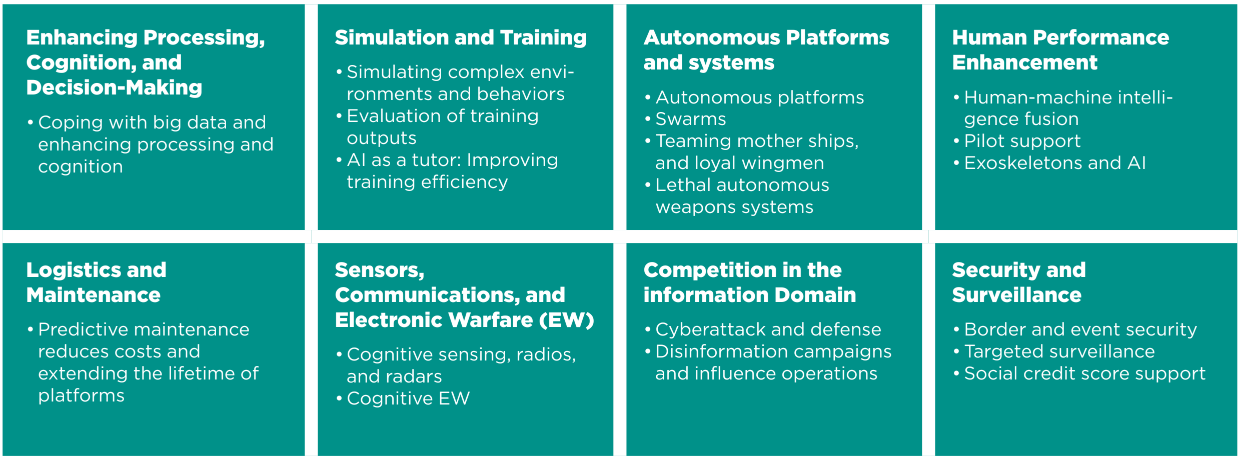
A FRAMEWORK FOR UNDERSTANDING APPLIED AI

Understanding this strategic geopolitical and security context and its implications is necessary to better assess the variety of ways in which AI technologies will be applied by the United States and its adversaries, as well as how these applications will shape the future of conflict, geostrategic competition, and military capabilities.

"Killer robots" and autonomous missiles chasing down unwitting or, possibly even unwarranted, targets tend to dominate the discussion of AI-enabled military and security capabilities and also tend to quickly turn to visions of Skynet from the Terminator films and battlefield singularities that pursue a military objective with ruthless efficiency and absent context, connection to commander's intent, or moral or ethical constraints.

Preoccupation with autonomous systems and weapons is not necessarily unhealthy or unwise. Continued development of lethal autonomous weapons systems (LAWS) and autonomous platforms poses real and complicated ethical and strategic questions unlikely to be resolved in the immediate future. So does the development of computer vision and facial and voice recognition systems that can be used to establish and advance a disturbingly efficient surveillance state.

However, the set of relevant applications of AI-enabled national security capabilities is much wider and, in many cases, more subtle than what is envisioned by a narrow focus on autonomous weapons or facial recognition. This paper has identified eight categories of AI-enabled operational capabilities that the United States, its allies and competitors, and even non-state actors are developing and deploying—or could be soon—in support of comprehensive national security objectives and enhanced military efficiency and capability.[46]



Enhancing Processing, Cognition, and Decision-Making

- Coping with big data and enhancing processing and cognition

Simulation and Training

- Simulating complex environments and behaviors
- Evaluation of training outputs
- AI as a tutor: Improving training efficiency

Autonomous Platforms and systems

- Autonomous platforms
- Swarms
- Teaming mother ships, and loyal wingmen
- Lethal autonomous weapons systems

Human Performance Enhancement

- Human-machine intelligence fusion
- Pilot support
- Exoskeletons and AI

Logistics and Maintenance

- Predictive maintenance reduces costs and extending the lifetime of platforms

Sensors, Communications, and Electronic Warfare (EW)

- Cognitive sensing, radios, and radars
- Cognitive EW

Competition in the information Domain

- Cyberattack and defense
- Disinformation campaigns and influence operations

Security and Surveillance

- Border and event security
- Targeted surveillance
- Social credit score support

Figure 1: A framework for bounding the ways in which AI-enabled capabilities are being applied in support of defense and security efforts by the DoD and other military and security communities throughout the world.

SOURCE: TATE NURKIN AND STEPHEN RODRIGUEZ

Analysis of activity in and across these categories reveals several cross-cutting themes about the value of AI for national security communities.

Terminology Matters. The discussion of AI for national security and defense is complicated by a lack of precision in language, specifically the tendency to conflate the terms—or at least the concepts—technology and capability. Articulating the relationship between them—and between capabilities, applications, and effects—is necessary for articulating the relationship between AI and the future of national security and military capabilities. Clarity in terminology, in turn, is important for devising an effective whole-of-government strategy to the development and deployment of AI-enabled capabilities in support of US national security and global stability, security, and prosperity.

Inventions in specific technologies expand the scope and scale of what is possible from an engineering or physics standpoint. AI is a general technology area roughly defined by its use of software to learn from exposure to data or its environments. Many specific AI techniques exist, as identified at the outset of this paper. Machine learning, deep learning, computer vision, and particle swarm optimization are all examples of the general technology area of AI.

Inventions and innovations in a specific technology do not constitute the development of a capability. For both state and non-state actors, moving from technological invention to a deployable capability requires coherent and creative operational concepts—a vision of how new technologies will be *applied* and what *effects* they will be deployed to achieve. For military and security communities, transiting this technology to capability pathway will also require change and innovation:

- new infrastructure development and changes to logistics and sustainment
- organizational, career, and cultural alignment
- establishing frameworks for addressing comfort of use/ethical issues
- changes to legal and regulatory environments to accommodate adoption and deployment of new technologies
- new procurement and industry engagement models that allow for the acquisition of novel technologies as they come available

The chain of innovation does not end with the development or deployment of capabilities. Capabilities are conduits through which new technologies like AI drive disruptive effects. This connection frequently gets lost in the discussion of AI in the context of a changed and still changing defense and security context. The endgame of AI development for any national security community is not the creation of an interesting new technology. Rather it is the creation of an effect that capitalizes on existing overmatch, mitigates vulnerabilities, or drives competitions in new and advantageous directions.

Strategic Value Framework. AI national security applications are employed to provide value at three levels:

> **Enabling Humans:** AI-enabled capabilities are designed to help operators, intelligence officers, and strategic decision makers prepare for ("readiness"), respond to, and operate more effectively in fast-moving and multidimensional strategic environments marked simultaneously by a surfeit of information *and* a high degree of uncertainty. The DoD Artificial Intelligence Strategy is largely focused on capabilities in this category that "augment the capabilities of our personnel by offloading tedious cognitive or physical tasks and introducing new ways of working."[47]
>
> **Removing Humans:** AI-enabled capabilities, especially in conjunction with unmanned systems and robotics, can be deployed to execute dirty, dull, or dangerous jobs such as counter-improvised explosive device missions, focusing humans on other less dangerous tasks.
>
> **Exceeding Humans:** National security communities are pursuing AI to catalyze the development and deployment of an entirely new set of nearly fully autonomous capabilities that have revolutionary processing power and decision-making speed, such as drone swarms, autonomous systems, and the ability to detect maliciously placed anomalies in images or maps. To paraphrase hockey great Wayne Gretzky, this category of capability development is designed to "skate to where the puck is going to be" in several years: to the commanding heights of cognitive warfare.

Going Big and Going Small. AI in the national security context is being developed first and foremost to better cope with the massive amounts of data and information being collected by nearly ubiquitous sensors, persistent social media platform monitoring, and the greatly increased availability of useful information in new media and other accessible open sources.

Machine and deep learning allow militaries to “go big” and more easily and rapidly collect and process data in order to develop a coherent situational awareness in a multidimensional, uncertain, and complex strategic and operational environment. These AI technologies also enable autonomous platforms and systems as well as manned/unmanned teams to consume multiple inputs quickly, autonomously adapting to changing circumstances. Going big has implications for readiness as well. Machine learning can improve the processing of decades of training results and after-action reports to better focus future learning curriculum, improving readiness as a result.

But AI applications are also designed to “go small”—to create tailored solutions that optimize the efficiency and effects of individuals or individual systems—reflecting the versatility of the technologies of interest to the national security community. Take, for example, using AI to develop customized training syllabi for individual students based on a small set of training interactions; or AI-enabled exoskeletons that adapt to each individual’s body and movements; or using data from ground vehicle fleets and individual platforms to establish predictive maintenance models for specific vehicles.

The Double-Edged Sword of Data. Access to more reliable data can lead to machine learning algorithms that perform better. Even over the relatively short history of DoD’s computer vision/object recognition effort known as Project Maven, accuracy improved with experience and exposure to more data.[48]

But the importance of data also confers competition for, and perhaps more importantly to the discussion of US strategy for AI and national security, vulnerability. Data is a critical point of failure for AI technologies. As such, it is an attractive target for both state and non-state actors to undermine US efforts to use AI to more effectively anticipate, deter, dissuade, degrade, and defeat the expanding range of threats to US security, stability, and prosperity. Corrupted or biased data can create algorithms that behave in unexpected or counterproductive ways, generating difficult to detect tactical, operational, and strategic challenges.

Ethics and Safety. Issues of ethics and safety go beyond even data corruption, which is an issue whose importance is difficult to overstate. But AI technologies themselves are neither good nor bad, and normative judgments about AI must be based on how the technology is employed, who is employing it, and for what purpose, more than a theoretical concept of what effects the technology could deliver. Individual technologies—facial recognition, for example—will have applications that sit at various points on the ethical spectrum, placing a premium first on reinforcing existing legal protections related to privacy and liberty, but also on establishing application and context-focused regulatory frameworks for determining the ethical use of AI in support of US national security.

In addition, ensuring that AI is “safe” and generates intended behaviors and outcomes is also critical to the effective and efficient incorporation of AI in any setting, but especially in national security and defense where the stakes can be particularly high. Creating reward functions for AI systems (and again ensuring the accuracy and completeness of data) that align human intent and machine action is an important component of AI development for national security.

Benefits of AI. It is easy to become consumed by the nuanced ethical issues surrounding AI and, in the process, lose sight of the benefits AI-enabled capabilities can provide for increasing advantages vis-à-vis competitors and also for defending the United States and its allies from novel AI-enabled threats.

NATIONAL SECURITY APPLICATIONS FOR AI

The list of national security applications of AI technologies is likely to expand beyond those included in the framework above as technologies mature and organizations become more deft at adapting these technologies. Ethics and safety issues will—and *should*—constrain some actors, including the United States. Key US competitors and non-state actors will be constrained more by the limits of human imagination than human ethics, meaning that the applications of AI for which the US national security community must prepare will expand as AI technologies mature, scale, and diffuse.

In the examination of each category, this paper explores why militaries and DoD specifically are interested in these individual AI applications and the effects they enable. The strategy paper also offers several examples of technologies and capabilities in development, including by commercial industry and applied research. The examples cited are indicative, not exhaustive, given the amount of accelerating and intensifying activity taking place in and across these application categories.

Intelligence and Decision-Making: Enhancing Processing and Cognition

The information revolution and deployment of pervasive sensors—both in operational environments and in everyday life—has greatly expanded the amount of useful information available to national security and intelligence communities. Dealing with this expanding and accelerating flow of information is overwhelming traditional manual processing efforts and soaking up a growing amount of the energy and effort of national security community personnel.

In a July 2017 speech to the Air Force Association in Washington, DC, United States Air Force Chief of Staff David Goldfein effectively captured both the challenges associated with manual intelligence processing in the information age and the promise offered by more complete integration of machine learning into intelligence processing and analysis activities.[49] Machine learning in the analysis of social media, for example, will reduce this burden by performing “that upfront analysis so that by the time it gets to the human level of analysis we’ve

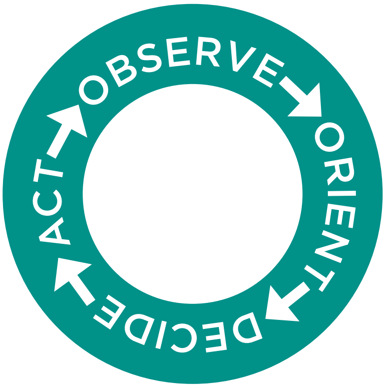


Figure 2: One of the most important and immediate security applications of AI is to speed up the OODA Loop (created by Colonel John Boyd USAF (ret.)), in response to fast-moving changes in the strategic and operational environment. AI technologies are particularly relevant to accelerating the first two elements of this process.

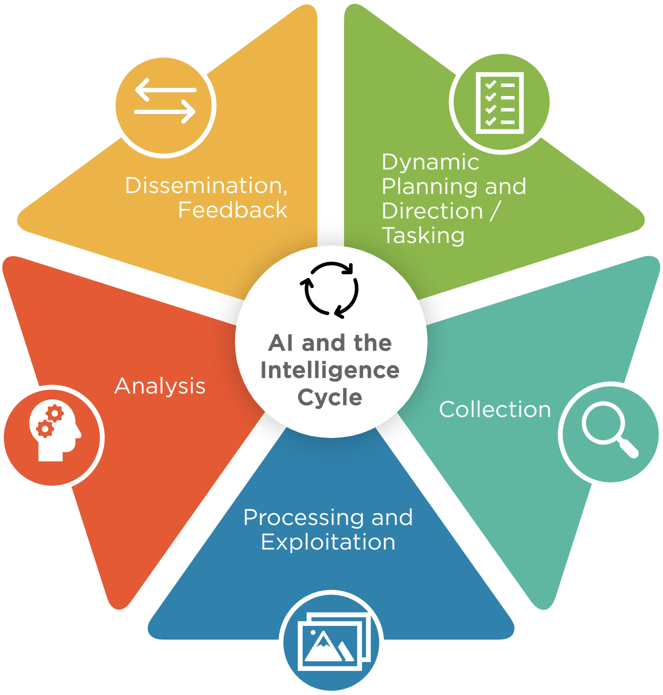
SOURCE: TATE NURKIN AND STEPHEN RODRIGUEZ

already refined it and focused it."[50]

Or, as a 2018 article coauthored by Lieutenant General Jack Shanahan (formerly head of Project Maven and now head of DoD's Joint Artificial Intelligence Center) and Cortney Weinbaum entitled "Intelligence in a Data-Driven Age" explained: "Artificial intelligence and machine learning provide opportunities to accelerate through every step of the OODA loop [see Figure 2] by making sense of data in real time as the data arrive, evaluating options and initiating an action in milliseconds, and acting . . . Machine learning offers new opportunities to shrink the first two phases of the OODA loop, greatly increasing the potential for humans to accelerate decision-making and taking action."[51]

DoD's Project Maven was the most high-profile effort aimed at incorporating machine learning processing of information into a human-guided process. The effort used computer vision to autonomously extract objects of interest from videos or imagery gathered by unmanned systems to enable humans to do "twice as much work, potentially three times as much, as they're doing now," according to Colonel Drew Cukor, the chief of the Algorithmic Warfare Cross Function Team within the Office of the Undersecretary of Defense for Intelligence.[52]

The project is most known for Google's 2018 decision to not renew the contract when it expired in 2019 due to ethical concerns of a large number of company engineers. Nonetheless, the program itself is reportedly set to go forward with another provider that will actually leverage an off-the-shelf Google Cloud Platform to support some workloads.[53] More importantly, the program is just the first step of what will be many DoD efforts to incorporate AI


Dissemination, Feedback
Dynamic Planning and Direction / Tasking
AI and the Intelligence Cycle
Analysis
Collection
Processing and Exploitation

AI can help identify patterns or anomalies that can support decision making

AI technologies such as facial recognition are contributing to collection activities

Intelligence cycle-related AI applications are currently focused on processing large amounts of data more quickly and more accurately than humans

Figure 3: The traditional intelligence cycle. AI is being deployed most prominently during the processing and exploitation (BLUE) stage.

SOURCE: TATE NURKIN AND STEPHEN RODRIGUEZ

into its intelligence processing workflow.

According to June 2018 comments from General James Holmes of the USAF Air Combat Command, AI-supporting intelligence processing "is a big part of our future and you'll continue to see that expanded." Project Maven was just among "the first steps in bringing learning machines and algorithms in to be able to allow people to focus on things that people do best and let the machine do that repetitive task."[54]

Keeping humans focused on things that people do best is key to optimizing AI's value across the stages of the traditional intelligence cycle, especially as machine learning and other AI technologies are integrated more prominently into this cycle [see Figure 3]. Intelligence tradecraft, alternative and structured analysis efforts, assumption challenging, and refined analytical filters will still be necessary for the dynamic and responsive tasking of machines and developing effective situational awareness. These skills and experience may even become more important in spotting data corruptions and offering feedback on how best to optimize the human-machine teaming in the intelligence cycle.

Training and Simulation

Closely related to AI enablement of improved human cognition is the use of AI technologies to support training and simulation efforts and, as a result, better decision-making and readiness.

From a training perspective, machine and deep learning are already offering means of developing highly customized training curricula for individuals. The US Air Force Air Education and Training Command (AETC) Pilot Training Next program's use of an AI trainer to evaluate not only student performance but also how each individual student learned led to thirteen of the twenty pilots that took part in the trial graduating in "half the time it normally takes to complete USAF's Air Force Specialized Undergraduate Pilot Training course."[55] The program is now seeking input from industry to improve machine learning algorithms and biometric sensors to better "keep pace with student progress."[56] In addition, deep learning is supporting training by analyzing the large amounts of data and after-action reviews generated by training exercises and war games over the course of the career of an individual soldier or larger unit.

But it is in AI-supported simulations where momentum and interest are especially strong, across the DoD and within other defense and security communities. The boost in simulation fidelity and complexity achieved through AI is seen as a strategic and operational discriminator, enabling defense and security communities to better plan for, deter, and respond to the complex and layered challenges of modern operating environments, hybrid warfare, and the integration of more advanced capabilities, *especially AI-enabled capabilities.* As the director of data science, models, and simulations for the U.S. Army's Training and Doctrine Command (TRADOC) noted in early 2018, "If we can marry big data and AI with [modeling and simulation] . . . that's an unbeatable advantage for not only the nation but our DoD and where we're trying to go. I'm really excited about the potential here."[57]

The recognition of the value of big data and AI applications can have for readiness is not only a US government or DoD phenomenon. Some defense communities are looking to AI and associated big data analytics tools to prepare for evolving, layered, and complex external threats to security and stability while other states are betting that AI-powered simulations will help overcome a strategically affecting lack of operational experience.

In September 2016, the European Defence Agency (EDA) launched a study known as Big Data in Defence Modelling and Simulation (BIDADEMS) aimed at better understanding how big data and deep learning could "potentially help to provide simplified military simulation designs, generate more realistic simulation scenarios and environments, improve the exploitation of simulation results or provide new opportunities for [modelling and simulation] M&S support to military test and evaluation (T&E) activities."[58]

The program led to a series of high-level recommendations that stressed incorporation of cloud computing, nonrelational databases, data analytics, and visual analytics into future modeling and simulation activities. It also led to a follow-on modeling and simulation program known as MODSIMMET that seems largely to be inspired by Russia's demonstrated capacity to exploit the fusing states of peace and conflict in Georgia, Crimea, and Ukraine. According to the EDA, MODSIMMET's focused objective was to use big data and AI-supported war games to better anticipate and manage "very complex scenarios like hybrid warfare."[59]

AI-enabled war-gaming and simulation models are of particular interest and utility to China, but for a different reason. China has not been involved in a military conflict since its 1979 war with Vietnam, and this lack of operational and command experience along with a rigid and centralized command structure are frequently cited as a vulnerability for China's military. That the United States has been at war since 2002 and presumably has learned from these experiences only magnifies this lack of experience and increases the need for more realistic AI-enabled war games and simulations.

China is also exploring simulations in which human operators compete against AI, an approach that allows human commanders an opportunity to develop new decision-making models based on AI player successes and failures. According to Elsa B. Kania, an adjunct senior fellow at the Center for a New American Security and a doctoral student at Harvard University, the China Institute of Command and Control cosponsored a national Artificial Intelligence and War-gaming Forum at National Defense University's Joint Operations Academy in September 2017. The exercise debuted a Chinese Academy of Sciences Institute of Automation-developed AI system called Prophet 1.0, which competed against humans in the exercise. The system defeated human teams "seven to one," providing useful data on what vulnerabilities in human decision-making the AI exploited and how and when these advantages were gained.[60]

Kania asserts that "going forward, the PLA's evident interest in the application of AI to war-gaming constitutes a notable direction of development" and that "these activities can produce data that is valuable to training AI systems for advances in war-gaming and novel techniques for decision-making."[61]

Autonomous Platforms and Systems

The most discussed application of AI for defense and security has traditionally been enhanced autonomy, including autonomy that over time will allow platforms and systems to respond and adapt to dynamic and complex environments either with greatly reduced human intervention or absent it altogether. Applications of AI in support of autonomous platforms and systems typically focus on four related areas: autonomous platforms, lethal autonomous weapons systems, swarms, and manned-unmanned teaming capabilities.

Autonomous Platforms and Lethal Autonomous Weapons Systems

The quest for heightened autonomy of individual unmanned air, ground, surface, and undersea vehicles has long been a priority for militaries (not to mention the automotive industry, further underscoring the connections between commercial AI development and emerging military requirements). At the end of the 2010s, many of the most advanced militaries in the world are coming closer to achieving this objective.

Reports of China's efforts to develop "large, smart, and relatively low-cost unmanned submarines that can roam the world's oceans to perform a wide range of missions"[62] and the March 2019 revelation of plans for a fully autonomous underwater base run by autonomous machines reflect the growing size and sophistication of autonomous platforms and the infrastructure required to support these assets. The US Navy request of over $400 million for two large Project Overlord unmanned surface vehicles to be purchased in 2020 is another example of this trend.[63]

As autonomous platforms become more viable in a broader range of missions, discussion of killer robots and the ethics of lethal autonomous platforms and weapons necessarily intensifies.

No defense or security application of AI is debated more across disciplines than lethal and fully autonomous weapons systems due to the immediate ethical concerns over removing humans from lethal OODA loops. Multiple groups of esteemed leaders in science, technology, business, and politics publicly expressed their disquiet about autonomous weapons citing the potential for a destabilizing AI arms race and the erosion of barriers for, as a 2015 letter signed by Stephen Hawking and Elon Musk noted, "tasks such as assassinations, destabilizing nations, subduing populations, and selectively killing a particular ethnic group."[64]

The United Nations has taken up the debate. In September 2018, the United Nation's Convention on Certain Conventional Weapons discussed an outright ban on fully autonomous weapons. The United States, Russia, South Korea, Israel, and Australia all thought the ban premature, suggesting a formal treaty on autonomous weapons systems should be informed by additional research into their potential security benefits.[65]

Despite resistance to banning LAWS, current US policy on autonomous systems is articulated through DoD Directive 3000.09, which requires that all weapons systems employ a "human in or on the loop" architecture.[66] Weapons platforms, such as fully autonomous weapons, that do not fall in either category are subject to a senior-level weapons review process.

However, in February 2019, the Army Contracting Command released a call to industry and academia to submit ideas to help build its Advanced Targeting and Lethality Automated System (ATLAS) ground combat vehicle. ATLAS will be designed to incorporate AI and machine learning to provide autonomous targeting capabilities enabling the system to "acquire, identify, and engage targets at least 3X faster than the current manual process."[67] The system is not thought to be fully autonomous as currently envisioned. The AI will be employed to speed up the "observe" and "orient" portions of the OODA loop, leaving more time in rapidly unfolding and high-pressure operational environments for humans to make decisions about what to target and when to fire.

Still, the announcement has reinforced concerns among many scientists, researchers, and industry about the slow and steady move toward fully autonomous weapons systems. Industry pushback forced the Army to release a revised call in March 2019 that included DoD-recommended language that emphasizes human control of lethal robots.[68] US competitors are unlikely to be similarly constrained, however.

Swarms

One of the most active areas of military AI research is in the development of autonomous swarms that consist of several to dozens or hundreds linked and networked unmanned systems, potentially operating across multiple domains: air, ground, sea, space, and cyberspace.

Individual systems within a given swarm will have specific functions—decoy, strike, air defense suppression, surveillance, electronic warfare—but all unmanned systems in the swarm will communicate with each other to carry out a mission. Humans may provide the broad parameters of the mission—identifying targets to be addressed, for example—and program the platforms, but the swarm will have the capacity to cognitively adapt to adversary countermeasures and a changing context.

Swarms are disruptive because they are autonomous, networked, and numerous. The combination of the ability to saturate air defenses, communicate and coordinate with one another to optimize mission performance, and autonomously adapt to changing operational environments allows swarms to be used in support of an exceptionally broad set of missions, including ground strike, intelligence, surveillance, and reconnaissance, and air-defense suppression, among others.

Both China and the United States have already successfully demonstrated military drone swarm technology—albeit at a relatively rudimentary technology-demonstrator level in uncontested environments. Among the growing number of examples, the US Air Force tested a swarm of 108 Perdix microdrones released from an F/A-18 Super Hornet in 2017[69] while China state-owned enterprise CETC tested a swarm of fixed-wing drones in June 2017.[70]

Other states are trying to catch up as the benefits of this AI-enabled capability become more evident and feasible. In February 2019, then-Minister of Defence for the United Kingdom Gavin Williamson announced that the UK would deploy "swarm squadrons" of drones by the end of 2019.[71] Williamson's apocryphal timeline has subsequently been corrected and extended out to the middle of the 2020s, but work on the concept continues. In April 2019, the MoD's Defence and Security Accelerator awarded a £2.5 million contract ($3.2 million) to further develop drone-swarming technology. The announcement came only weeks after the MoD announced a £31 million investment in minidrones, to include minidrone swarms.[72]

A more tangible and immediate example of the diversity of drone swarm programs and pace of their development was seen at the November 2018 Zhuhai Air Show, China's premier defense exhibition. Among multiple swarming concepts demonstrated at the show was China North Industries Corporation's (NORINCO) tactical concept for the use of swarmed strike-capable, multirotor unmanned aerial vehicles (UAVs), according to *Jane's Defence Weekly.* The UAV swarm was advertised as being effective against multiple targets, including "armored vehicles, artillery systems, radar, military and storage facilities, communication hubs, aircraft shelters, and logistics support lines."[73]

The AI, communications, and electronic warfare (EW) defense technologies and operational concepts behind drone swarms need to develop in order for swarms to operate in contested environments. However, successful demonstrations of UAV and unnamed surface vehicle (USV) swarms and mounting interest in the capability suggest a highly prioritized "skate to where the puck is going to be" capability. As one engineer who supported a record-setting June 2017 test of a swarm of 119 swarmed drones by CETC noted to China state-run media, swarms "will change the rules of the game."[74]

'Loyal Wingmen' and Manned-Unmanned Teaming

Research on autonomous systems has facilitated development of new capabilities and applications that pair manned and autonomous unmanned ground, air, surface, and undersea platforms and systems.

In the air domain, DoD has considered the "loyal wingman" concept for several years, including an approach that would pair a manned F-35 with unmanned F-16s with sufficient autonomy to "complete all basic flight operations untethered from a ground station and without full-time direction from the manned lead."[75] More recently, the US AFRL has unveiled two low-cost attritable[76] UAV technology demonstrator programs—Skyborg (Boeing) and Valkyrie (Kratos)—that incorporate different degrees of autonomy in support of manned aircraft.[77] In May of 2019, DARPA briefed industry on a similarly scoped program known as the Air Combat Evolution (ACE) program. ACE will enable one human pilot to "become a more deadly warfighter by leading several semiautonomous artificially intelligent unmanned aircraft, all from his own cockpit."[78]

Human Performance Enhancement

Developments in AI technology are intersecting with progress in other 4IR technologies such as neuroscience, bioscience, virtual and augmented reality, smart materials, and robotics to capitalize on the fusion of the physical and digital, of humans and machines. The objective? To improve the cognitive capacity of individual operators; advance the ability of humans to interact with machines; and provide additional endurance, recovery, healing, physical capacity, and safety.

Machine-Human Intelligence

In 2015, Ray Kurzweil, the chief engineer at Google, predicted that, by 2030, humans would be "hybrids," meaning that the human brain would be connected to the cloud and, as a result, "our thinking then will be a hybrid of biological and non-biological thinking."[79]

Among, DoD's efforts at understanding and unlocking the potential of machine-human intelligence is DARPA's OFFensive Swarm Enabled Tactics (OFFSET) program, which is pursuing solutions for small military units operating in urban environments to work closely with swarms of up to 250 drones.[80] Desired outcomes are ambitious, but reflective of the potential of AI to increase squad effectiveness through enhanced human-swarm teaming, including: "interface modalities such as pan and touch, gestures, or even speech for intuitively conveying commander's intent through swarm tactics."[81]

Of course, the United States is not the only country interested in the intersection of machine and human intelligence. On October 10, 2018, at the Association of the US Army (AUSA) Exhibition in Washington, DC, Lieutenant General Robert Ashley, the director of the US Defense Intelligence Agency (DIA), suggested that China's efforts to use neural nets to teach machines to think is part of a process that will inevitably include "the integration of human and machines."[82] China's government is already funding academic research in this area, according to Kania: "The PLA's Academy of Military Science has focused on advancing military-civil fusion . . . in brain science research, including to explore options to enhance human capabilities for battlefield perception and decision-making."[83]

Exoskeletons and AI

Exoskeletons are wearable technologies that help individual soldiers reduce fatigue and enhance endurance, safety, and strength. The US and Russia are considered global leaders in exoskeleton development, and the Russian EO-1 passive exoskeleton was reportedly used in Syria in March and April 2017 to support mine-clearing operations in Palmyra.[84]

The US Army is seeking to gain advantage in this competition and more importantly develop a capability that can enhance warfighter performance by building in AI that will make exoskeletons responsive to the parameters of individual bodies and movements.

In late November 2018, the US Army Natick Soldier Research Development and Engineering Center awarded a two-year, $6.9 million contract to Lockheed Martin to further develop the ONYX exoskeleton system. ONYX is a powered, lower-body exoskeleton that uses electromechanical knee actuators, a suite of sensors, and an AI computer to boost human strength and endurance.[85] Keith Maxwell, exoskeleton technologies program manager at Lockheed Martin, is quoted by *Defense One* as saying that the AI "is learning the soldier's gait. The longer the [soldier] is in the system, the system optimizes to push him along through that process."[86]

More progress is being made in academia in demonstrating the value of using AI in exoskeletons to make the systems tailorable and more efficient. Researchers at Harvard University are developing "a soft exosuit" that helps individuals move with minimal effort. The system embeds AI to sync machine and human movements and to make sure the suit is tailored to each individual. There is no evidence that Harvard's research is focused on military or security applications—the medical and health care industry as well as other sectors that require physical exertion and lifting also have understandable interests in the technology. Clearly DoD will be interested in developments emanating from this and related academic and industry research.

Logistics and Maintenance: Predictive Maintenance

AI has significant potential to improve maintenance, repair, and overhaul activities by identifying impending problems in equipment before they occur, reducing maintenance costs, and increasing readiness.

Predictive maintenance uses AI software to accumulate data from sensors and monitor anomalies during routine functioning to determine issues and request human input or intervention.[87] As with exoskeletons, one of the main values of predictive maintenance is customization—in this case of maintenance and repair models. Data collected across entire fleets of thousands of individual vehicles are the foundation for predictive models, but these models are further refined based on data taken from each individual platform, which will have its own operations history and therefore unique maintenance needs.

DoD's focus on predictive maintenance was highlighted in the recently released AI strategy document, which included a specific mention of "implementing predictive maintenance" as one of three examples of priority areas for AI incorporation into DoD mission areas. The document also included examples of how predictive maintenance applications are supporting US forces and driving efficiencies. According to the strategy document, "The Defense Innovation Unit (DIU) and the US Air Force are working together and with the JAIC to produce prototypes of Predictive Maintenance solutions and to scale successes. These commercially developed AI-based applications have the potential to predict more accurately maintenance needs on equipment such as the E-3 Sentry, F-16 Fighting Falcon, F-35 Lightning II, and Bradley Fighting Vehicle, thereby improving availability and reducing costs."[88]

Cognitive Sensing, Communications, and Electronic Warfare

The ability of the US military to freely operate and access the electromagnetic spectrum is critical to its overall ability to deter and dissuade challenges, competitor and adversary risk-taking, and to defeat adversary forces if necessary.

As former Chief of Naval Operations Admiral Jonathan Greenert described in 2016:

> *The electromagnetic spectrum is an essential—and invisible—part of modern life [military and civilian]. Our military forces use wireless computer networks to coordinate operations and order supplies, use radars and sensors to locate each other and the enemy, and use electronic*

> *jammers to blind enemy radars or disrupt their communications. With wireless routers or satellites part of almost every computer network, cyberspace, and the electromagnetic spectrum now form one continuous environment.*[89]

This "essential—and invisible"—environment has become increasingly *congested and contested* over the last decade, driving demand for new capabilities that can sense and diagnose challenges to efficient use of the electromagnetic spectrum.

AI-enabled cognitive radar, sensors, and radios are able to intelligently detect traffic on *congested* bandwidths and autonomously adapt to achieve superior performance in functionality, whether that is detection, tracking, or transmission.

One mission-critical example of cognitive capabilities—in this case bandwidth management—is seen in the National Institute of Standards and Technology (NIST) efforts to use AI to better monitor use of the primarily military bands. Commercial companies seek to leverage the 3.5 gigahertz band but are required to yield when military requirements are high. Detecting when offshore military assets like ships are operating—and therefore when commercial companies must yield—can be a challenge. Currently used energy detectors are "not discriminating enough to consistently get it right, sometimes confusing other radio frequency signals as radar or missing the radar signatures altogether."[90] According to NIST research, AI algorithms "appreciably outperformed the energy detectors" in determining when this high-value band would be open and for how long.[91]

Cognitive Electronic Warfare

Cognitive electronic warfare (EW) capabilities are also helping the DoD better operate in a *contested* electromagnetic (EM) spectrum.

China and Russia have developed more advanced EW weapons that challenge US capability to operate freely across the electromagnetic spectrum. Russia's efforts to jam Global Positioning System (GPS) signals between October 16 and November 7 during NATO's 2018 Trident Juncture exercise in Norway[92] is indicative of the open competition playing out in the EM spectrum.

Cognitive EW is DoD's answer to managing the escalating EW threat. Cognitive EW programs, such as DARPA's Behavioral Learning for Adaptive Electronic Warfare[93] and Georgia Tech Research Institute's Angry Kitten program, use machine learning to allow EW systems to observe a threat system and then characterize that adversary system "on the fly." Once characterized, the machine learning system is able to then devise and deploy a countermeasure in real time. Cognitive EW can also perform EW-related battle damage assessment and alter its countermeasures based on adaptations in the adversary's radar or EW activities.[94]

Competition in and Exploitation of the Information Domain: Cyber Security and Deepfakes

Cyberattack and Defense

The intersection of commercially available and easily diffused AI technologies and the reliance on the information/cyber domain is particularly concerning for defense and security planners. AI-infused cyber threats can be exceptionally difficult to detect, attribute, and deter through the traditional means of "military-technological overmatch."

In February 2018 researchers at seven think tanks and universities, including Oxford and Cambridge universities, the Center for New American Security, and OpenAI, released a report entitled "The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation." The report argued that "the use of AI to automate tasks involved in carrying out cyber-attacks will alleviate the existing trade-off between the scale and efficacy of attacks. This may expand the threat associated with labor intensive cyber-attacks."[95]

By incorporating easily diffused AI software, cyber operations have the potential to be in a constant state of rapid attack, "seeking to penetrate as many networks as possible and then lie in wait for strategic moments of exploitation."[96]

Perhaps even more worrisome is the prospect of targeted machine learning-fueled cyberattacks that autonomously avoid even state-of-the-art defenses and remain dormant until they reach a specific target, which itself may be identified through AI applications such as facial or voice recognition.

Targeted cyberattacks are not new, but what is alarming about modern tailored cyberattacks is just how accessible the software required to craft them has become. At the Blackhat USA 2018 Conference, International Business Machines Corp. (IBM) revealed its DeepLocker effort to test the effectiveness of a deep neural network-enabled targeted malware. The IBM team used a hacked version of a videoconferencing software that used AI-supported malware to avoid detection and to exhibit "benign behavior" at nontargets.[97] It only released its malware when it detected the face of the target, using facial recognition software embedded in the malware. IBM listed a series of other attributes that such malware could be trained to detect to determine its target, such as audio, user action, geolocation, software environment, sensors, and physical environment.

"We have a lot of reason to believe this is the next big thing," DeepLocker research head Marc Ph. Stoecklin is quoted by Reuters as saying. "This may have happened already, and we will see it two or three years from now."[98]

But the news is not necessarily all bad for those concerned about the intersection of AI and cyberconflict. First, the policy focus should be on ensuring AI use does not continue to make cyberspace an offensive-dominated environment. Machine learning and deep learning can serve in a cyberdefense role as well, particularly in iteratively and more rapidly reviewing network data to identify, classify, remediate, and mitigate vulnerabilities. In fact, the IBM DeepLocker team's suggested remedies for "AI locksmith" attacks included AI-based solutions such as "AI usage monitoring" and "AI lockpicking." Vulnerabilities will persist, but speeding up the pace of identifying these vulnerabilities will be a highly salient area of use for AI (and specifically machine learning) systems. Second, the democratization of cyberspace and adoption of AI applications will increase the number of nefarious actors. US AI policy should emphasize threat management by US agencies at risk of being overwhelmed by attacks.

Ultimately, even though AI applications for cybersecurity are still maturing, AI is, as one technology industry expert noted, "transforming the industry, and we can expect to see a number of trends come to a head, reshaping how we think about security in years to come."[99]

Exploitation of the Information Domain: Disinformation Campaigns, Influence Operations, and Deepfakes

AI also provides tools that will greatly enhance the capacity of actors to design, target, and deliver focused and tailored disinformation campaigns and influence operations. AI researcher and blogger Francois Chollet believes the most worrying application of AI technologies is "the highly effective, highly scalable manipulation of human behavior that AI enables, and its malicious use by corporations and governments . . . This risk is already a reality today, and a number of long-term technological trends are going to considerably amplify it over the next few decades."[100] Lieutenant General Shanahan and Weinbaum raise this concern as well, arguing that "widespread integration of machine learning and AI will present new opportunities for deception resulting from data that have been altered or manipulated. Counter-AI will become prevalent while influence operations will take on new dimensions that have yet to be fathomed."[101]

The USG—well-beyond DoD—views deepfakes as a particularly worrisome application of the deceptive and manipulative use of deep learning, given the political and societal fissures in the United States and its allies that other competitors have already exploited.

Deepfakes can be used to create realistic face and/or voice swaps in images or videos. AI is used to help stitch the replacement image onto the original. Imagine videos of political figures saying or doing things that they did not say or do being injected into a world in which distinctions between reality and perception are not relevant, in which facts have given way to preferred interpretations.

This is not a distant hypothetical. University of Washington researchers were able to create a "synthetic Obama" in 2017 using neural networks to model the former President's mouth and then mapped their model to fourteen hours of footage and audio of Mr. Obama to capture voice and mouth movements. The synthetic Obama was able to say anything that the real Obama had said in those fourteen hours of audio as well as to say anything an impersonator could say, opening up the possibility for the use of this technology to release intentionally misleading or distorted statements from any political leader.[102] A doctored video of House Speaker Nancy Pelosi in which she appeared to stumble drunk while slurring words was a relatively unsophisticated version of this cognitive attack, yet still attracted national attention in May 2019.[103]

In September 2018, US Representatives Carlos Curbelo (R-FL), Stephanie Murphy (D-FL), and Adam Schiff (D-CA) sent a letter to then-Director of National Intelligence Dan Coats urging US intelligence agencies to investigate the rise of deepfake photos and videos that "malicious foreign or domestic actors" would be able to use to easily spread misinformation and propaganda. According to the letter, "by blurring the line between fact and fiction, deep fake technology could undermine public trust in recorded images and videos as objective depictions of reality." The problem of deepfakes is troubling enough that Google is working with DoD to better understand ways to determine whether a picture or video has been tampered with.[104]

As with targeted cyberattacks some of the building blocks for deepfakes are no longer the exclusive property of nations or even commercial organizations. Among the many deepfake apps now available commercially is FakeApp, which leverages face-swapping algorithms to help anyone who can download the app to manipulate actual video or voice footage or photos for whatever motive—whether it be humor, revenge, extortion, or political influence and disruption. A quick search on YouTube brings up links to several tutorial videos on how to install and use FakeApp and other deep-fake apps.

Indeed, recent reporting indicates criminal groups are incorporating deepfakes. According to the Wall Street Journal, in March 2019, a British energy company's executive wired €220,000 ($243,000) purportedly to a supplier in Hungary at the apparent urgent request of his boss.[105] The request came via a phone call that used an AI-based software that imitated the sound of the executive's boss's voice, "and not only the voice: the tonality, the punctuation, the German accent."[106] The money was wired to a Hungarian bank and has since been transferred to Mexico and other locations throughout the world.[107]

Adversarial Examples

Adversarial examples are inputs to machine learning models and neural networks that an attacker has intentionally designed to cause the model to make a mistake. Artfully crafted adversarial examples are particularly challenging not only because they generate "optical illusions for machines,"[108] but also because the disconnect between the physical world reality supposedly being captured in an image and the manufactured perception the adversarial example has created is extremely difficult for either humans or machines to detect. Adversarial examples actually exploit the ways in which neural networks "see" and identify images.

The disruptive applications of adversarial examples are myriad. In a strictly military context, they can trick a neural network into seeing physical objects or aspects of landscape that do not exist or are, in fact, something else. At a tactical and operational level, the advantages conferred by the ability to change the images of the physical landscape on which military planners rely are clear: creation of features that do not exist, such as bridges, can alter tactical decision-making while shifting the nature of a building from, say, a hospital to a military target, with potentially devastating human and strategic consequences.

Moreover, the use of adversarial examples outside of the explicitly military or security context could pose precisely the sort of threats to the faith in government's ability to keep up with modernity that are appealing in a world in which states of peace and conflict are fusing. As Todd Myers, automation lead for the CIO-Technology Directorate at the National Geospatial-Intelligence Agency, was quoted as saying by Defense One in March 2019: "Imagine Google Maps being infiltrated with [adversarial examples], purposefully."[109]

Security and Surveillance

In his 1962 Rice University speech articulating US commitment to putting a man on the moon by the end of the 1960s, President John F. Kennedy Jr. rightly claimed that "space technology, like nuclear technology and *all technology* [emphasis added], has no conscience of its own."[110]

For all of the considerable scientific and technical appeal and potential benefits which AI technologies can bring to the pursuit and maintenance of stability, security, and prosperity, many of the applications of AI bring with them both immediate and longer-term ethical challenges and implications.

Much like LAWS, applications of AI for security and surveillance can straddle the ethical AI line, falling on one side or the other largely based on:

- the context and purpose of the employment of AI technology;
- the identity of the organization employing it;
- whether and how collected data are stored and who has access to that data and under what circumstances;
- who the technology is deployed to monitor;
- the quality of the technology itself; and
- whether individuals know they are being monitored.

Implementation of facial recognition software offers a useful example. In late 2018, *Rolling Stone* magazine reported that pop music artist Taylor Swift had used facial-recognition software outside of her concert at the Rose Bowl. The camera was embedded in videos of Swift's rehearsals playing at a kiosk set up at the entrance of the stadium and was used to identify known stalkers. Images of everyone who looked at the footage was sent back to a security command center in Nashville, Tennessee, and cross-referenced against an existing database of individuals previously identified as Swift stalkers. Data associated with images that were not matches were reportedly not retained, meaning that only data pertaining to individuals previously identified as stalkers were retained.[111]

Even in this context, there was alarm that the monitoring was done in secret—meaning that no one attending the concert was aware that his or her image was being scanned and reviewed. There is also concern that facial recognition as part of event security could be used by law enforcement to identify persons of interest in totally unrelated cases. During the 2001 Super Bowl, for instance, facial recognition software identified nineteen attendees with outstanding warrants.[112] That none of those individuals were subsequently arrested as a result of the software did not assuage fears about facial recognition dragnet operations.

The European Union's (EU's) Intelligent Border Control initiative (iBorderCtrl) offers another example of the nuance associated with implementation of these systems. The trial program uses "intelligent border guards" to support vetting of individuals entering three countries-—Latvia, Hungary, and Greece.[113] The system's most prominent feature is an avatar that asks a traveler from outside the EU a series of questions. "The AI software looks for subtle symptoms of stress as the interviewee answers. If enough indicators are present, the system will refer the traveler to a human border guard for secondary screening."[114]

The system is most immediately and directly a response to concerns about the expanding and intensifying range of border security challenges in Europe. As George Boultadakis, project coordinator of European Dynamics in Luxembourg, is quoted on the European Commission website, "The global maritime and border security market is growing fast in light of the alarming terror threats and increasing terror attacks taking place on European Union soil, and the migration crisis."[115]

As with the use of facial recognition for event security in a liberal democracy, there are significant comfort of use issues for iBorderCtrl and other applications for point-of-entry security:

- **robustness of legal protections**—in place to ensure safe and ethical use
- **bias**—the system cannot discriminate or mischaracterize expressions or voice intonation based on race or other inherent factors
- **the fate of the data**—destroyed is preferable to retained and if the data are retained there should be strict regulations about access and use
- **the context of use**—point-of-use is preferable to extensive, pervasive, and omnipresent
- **targets**—based on previously demonstrated illegal or suspicious behaviors would be generally preferable to AI that targets specific minority groups or all citizens in anticipation of or to track possible suspicious or "unpatriotic" behavior

The application of many of the same types of AI technologies at scale by the CCP for domestic security and surveillance purposes creates a different response compared with many liberal democracies.

Reports of the use of facial recognition software across China, including in railway stations in Beijing and other major cities, as well as leveraging big-data analytics to help scour huge datasets to support the development of social credit scores are common.[116]

AI-fueled domestic surveillance is especially prominent in Xinjiang,[117] and compulsory collection of Uighur biometric data has provided a larger and more accurate database that can be leveraged to identify and monitor this ethnic group.[118] The *New York Times* reported in April 2019 that "documents and interviews show that the authorities [in China] are also using a vast, secret system of advanced facial recognition technology to track and control the Uighurs." The combination of different types of AI technologies and big data analytics allows Chinese authorities to detect departures from "normal" behavior among Muslims—and then to identify each supposed variance for further state attention.[119]

This sort of wholesale collection of sensitive personal data—both in China and elsewhere as the technology proliferates—furthers Orwellian visions of the future of the polity's control of society. It also expands the vulnerability of individuals to manipulation by non-state actors through the cyber-theft of biometric data. This cyberrisk was realized in February 2019 when a Dutch cyberresearcher revealed that Chinese facial recognition company SenseNets had accidentally released a database with facial recognition and other personal data collected through its software's use in China.[120]

The use of AI for wide social surveillance and manipulation and as an instrument of political control constitutes a challenge to US values and ultimately to US interests and national security. The implications for US national security are magnified, though, by China's proactive efforts to export AI-supported systems that have become so central to its own domestic surveillance and security efforts. In April 2018, the *Global Times* reported that the Chinese company Cloudwalk had signed a strategic cooperation framework agreement with the Zimbabwe government to export facial recognition technology as part of China's Belt and Road Initiative. The deal includes support of development of generally beneficial systems such as a smart financial-service network. Cloudwalk will also help "introduce intelligence security applications at airports, railways, and bus stations" and, of most concern, "build a national facial database in Zimbabwe."[121]

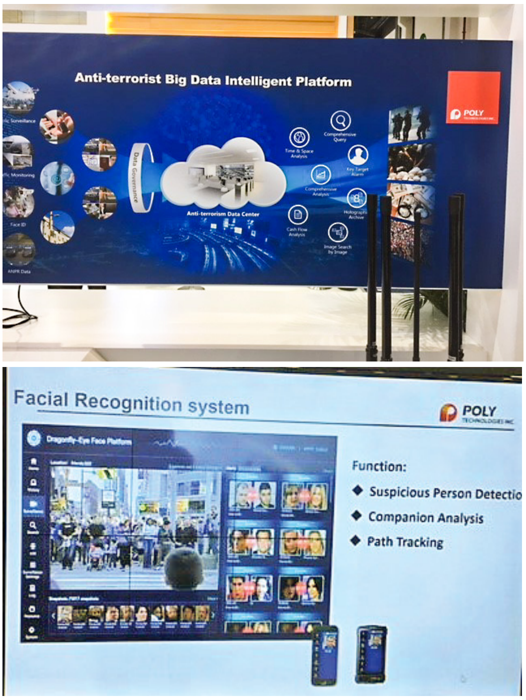


Figure 4: Big data analytics and facial recognition systems are being marketed at international defense exhibitions by Poly Group, a Chinese state-owned.

SOURCE: TATE NURKIN

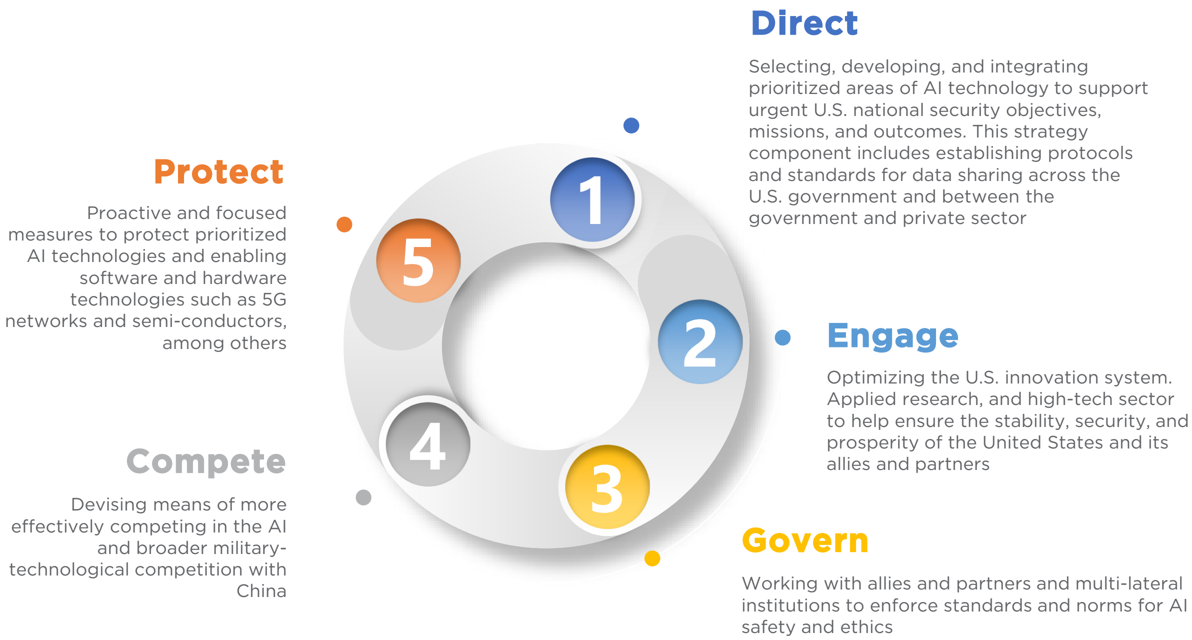
IVARS UTINĀNS/UNSPLASH

GOALS AND ELEMENTS OF THE STRATEGY

The release of DoD's AI strategy and the president's executive order in February were welcome developments, recalling the flurry of government activity on quantum computing in September 2017. The AI announcements reflect a growing sense of urgency and purpose in developing US AI strategy in support of US security and prosperity.

Now is the time to build on this momentum by connecting and aligning the AI development approaches and initiatives across the US national security community and government and identifying specific actions and objectives for achieving the executive order's vision for sustaining US advantage in AI development and exploitation.

The strategy recommended in this document is built around five components: direct, engage, govern, compete, and protect. These components are not unconnected. They overlap and intersect—in some areas quite significantly. Measures to protect US technological advantage will support whole-of-government engagement with the US (and global) high-tech industry and is also an important element of US efforts to meet China's geopolitical and AI competitive challenge. Being the global leader in AI ethics and safety—the main thrust of the govern component—supports US competitive efforts vis-à-vis China as well.



Direct

Selecting, developing, and integrating prioritized areas of AI technology to support urgent U.S. national security objectives, missions, and outcomes. This strategy component includes establishing protocols and standards for data sharing across the U.S. government and between the government and private sector

Engage

Optimizing the U.S. innovation system. Applied research, and high-tech sector to help ensure the stability, security, and prosperity of the United States and its allies and partners

Govern

Working with allies and partners and multi-lateral institutions to enforce standards and norms for AI safety and ethics

Compete

Devising means of more effectively competing in the AI and broader military-technological competition with China

Protect

Proactive and focused measures to protect prioritized AI technologies and enabling software and hardware technologies such as 5G networks and semi-conductors, among others

Figure 5: The five components of an AI strategy for national security.

SOURCE: TATE NURKIN AND STEPHEN RODRIGUEZ

GOALS OF THE STRATEGY

Across all five components, this strategy stresses USG leadership, a more risk-tolerant approach to incorporating AI into national security efforts, and proactive engagement between government agencies and with the US private sector, allies, partners, and the international community. The strategy is designed to achieve three main objectives:

- facilitate conditions and articulate guidance that will optimize the outputs of the US innovation ecosystem and high-tech industry in developing safe and trustworthy AI for the benefit of US security and prosperity
- strengthen the United States and its allies in the global competition to develop and deploy advanced AI, especially in the US military-technological competition with China
- influence global development and, particularly, deployment of AI-enabled capabilities along a trajectory that is consistent with core liberal democratic values, principles, and priorities, namely maintenance of individual liberty, rule of law, privacy, and fairness

Specific recommendations are a mixture of actions the USG should **stop** taking, current approaches that the USG should **continue,** and new or enhanced approaches or information and analysis the USG should **begin** or **create,** especially in support of filling in knowledge gaps about AI development in the United States and among allies and competitors.

DIRECT

“Direct” Summary and Recommendations

President Trump’s executive order did not provide the specific guidance or direction on which AI-enabling technologies and, more importantly from a national security perspective, applications of these technologies, should be prioritized for funding.

We recommend the following actions to support *prioritization and integration* of novel AI technologies and government facilitation of more *open sharing of data* across government as well as with the private sector:

Prioritization

- Align technology and capability priorities to ensure the security, stability, and prosperity of the United States, using an effects-focused framework
- Invest in and protect AI-enabling technologies
- Develop an interagency survey to first understand and then leverage overlaps between AI priorities for national security and other government priorities.

Integration

- Improve training and education about AI within the US national security community
- Form a Data Integration Task Force led by the chief data scientist out of the Executive Office of the President

Data Access

- Go beyond the Foundation for Evidence-Based Policy Act
- Adapt—not adopt— the EU’s General Data Protection Regulation (GDPR)

Prioritization of AI Technology, Capabilities, and Effects

President Trump’s February 2019 executive order was viewed by many policy makers and lawmakers as essential for laying the groundwork to capitalize on everything from national 5G communications, fusion with autonomous vehicles, and addressing emerging national security requirements.

It was hailed in some communities as the AI strategy for which policy makers and practitioners had been waiting, even if it lacked specificity, and ultimately, effective direction.

Daniel Castro, the director of the Center for Data Innovation, was quoted by the *Federal News Network* as welcoming the executive order, but urging the White House to “do more than reprogram existing funds for AI research, skill development, and infrastructure development . . . it should ask Congress for significant funding increases to expand these research efforts."[122] The executive order was more of a proclamation that served notice that the United States intended to expand and, at some point, focus efforts to support R&D of AI capabilities and devise approaches for mitigating the risks associated with this development.

One thing it did not do is provide specific funding for agencies, though it did direct senior leaders to guide existing Fiscal Year 2020 R&D funding toward White House priorities. The executive order,[123] and the American AI Initiative it launches, lays out six strategic goals for agencies:

- promote sustained investment in AI R&D with industry, academic, and international partners
- improve access to high-quality and fully traceable federal data
- reduce the barriers to greater AI adoption
- ensure cybersecurity standards to minimize vulnerability to attacks from malicious actors
- train the next generation of US AI researchers
- develop a national action plan to protect the advantage of the United States in AI

The lack of guidance on funding and paucity of content that describes exactly how the White House and the USG as a whole should execute the new strategy leaves important unanswered questions. One such foundational question was raised by Kelvin Droegemeier, the new head of the White House's Office of Science and Technology Policy (OSTP), when speaking at the American Association for the Advancement of Science following the release of the executive order. According to *Federal News Network* reporting, Droegemeier thinks implementation of a broad interagency approach to AI research and development for national security would require a far better understanding of *the current state* of that research within the United States. The USG doesn't have a clear headcount of how many researchers and institutions are actually working on AI across the government, the private sector and nonprofit sectors, according to this reporting, which says Droegemeier highlighted that the portfolio of AI-related fields covers everything from computer science and applied mathematics to industrial engineering, psychology and ethics.[124]

Another gap in the executive order is the absence of bureaucratic mechanisms to ensure the interagency coordination that is mandated. The president can establish his intent but without incentives to comply, agencies will continue to follow their own vision. Here, the Pentagon has shown strong leadership with its own implementation plan supported by allocated funding for AI development and a growing bench of expertise. The establishment of the JAIC, the organization's early efforts to engage academia and industry and "facilitate collaboration across the DOD," and its focus on immediate priority national-mission initiatives such as cyber are reflections of the Pentagon's leadership in this area.[125]

These actions, while not amounting to a strategy in and of itself, are the highwater mark for agency progress across the government. The rest of the government mirrors the executive order's tenor in its AI direction; that is to say, guidance without process or allocation of resources.

To fill this current gap in specific direction for AI investment and development in support of US national security, the authors of this report recommend:

- **Aligning investment priorities with key domain area competitions.** The alignment of AI investment should be based on a clear understanding and articulation of the prioritized threats, missions, and disruptive effects the US needs to achieve to enhance the security and prosperity of the United States.

  Priorities would align roughly with the eight capability areas identified above with a particularly acute focus on:

  - using AI technologies to better address the growing and potentially highly disruptive and layered challenge posed by AI-generated deepfakes and other AI-enabled disinformation campaigns as well as offensive cyberattacks;
  - deploying machine learning to support the processing of the abundance of information available to intelligence analysts, decision makers, and operators;
  - developing AI-enabled cognitive electronic warfare capabilities to maintain superiority in the invisible but important electromagnetic spectrum;
  - utilizing AI across training and predictive maintenance applications to improve readiness of individuals and units to meet fast-moving threats and cope with multispectrum operating environments; and
  - developing autonomous ground, air, surface, and undersea assets and the concepts and key technologies that enable greatly enhanced human-machine teaming.

- **Analyzing and mapping US innovation ecosystem.** In April 2017 the White House ordered a thorough review of the US defense industrial base as a first step in developing the relationships, capabilities, protections, and incentives to enhancing US national security and maintaining advantage in military-technological competition, especially with China. The study reportedly identified over "300 vulnerabilities,"[126] and, as a result, priorities for mitigation and redress, and further investment.

  As the traditional defense industrial base collides with high-tech, automotive, energy, maritime, and commercial aerospace industries as well as applied research communities, the government will need a more complete understanding and mapping of this powerful, but disparate and in many ways disconnected, innovation base to accompany analysis of the defense-industrial base. The USG needs to determine and then monitor "who is working with whom on what?" The American private sector already funds more basic research that the USG with academic basic research doubling since World War II. Developing a better sense of where this investment is going will be critical to helping the government identify priorities for a portfolio approach among the private sector, academia, and the government to support future codevelopment of dual-use, AI-enabled capabilities that can support US national security.

Consequently, we recommend a biennial evaluation of the US research and development ecosystem that optimizes research priorities, planned funding levels, and enabling partnerships between US and foreign research entities.

- **Focusing on amplifying technologies.** Success in AI development—in an absolute sense and in relation to China and Russia—will rely in part on the US ability to establish and maintain advantage, or at least competitiveness, in several science and technology areas that individually and collectively amplify the effectiveness of AI-enabled capabilities. Fifth-generation (5G) networks, quantum computing and encryption, semiconductors, neuroscience and bioscience, robotics, unmanned systems, and cloud computing all stand out as strategically crucial science and technology areas that are intersecting with AI development for national security and defense.

  Some of these, such as 5G, quantum computing, and semiconductors, are notable because they increase bandwidth and processing speed sufficiently to allow for faster and more powerful calculations, learning, and decision-making. Other areas, like unmanned systems and neuroscience and bioscience, create new or enhanced ways in whcih AI can be deployed in support of military missions or national security objectives. Regardless of the specific supporting function of the enabling technology, though, competition between the United States and China is intensifying in each of these technology areas, as demonstrated by US efforts to ban Huawei from its incipient 5G architecture and to pressure allies and partners to follow suit. In some areas, particularly 5G and possibly quantum computing, Chinese manufacturers and engineers are likely ahead of the United States in deployment of technology-enabled capabilities. In other areas such as unmanned systems, China has achieved high-profile and easily validated successes that indicate a high degree of competency and a closing of the technological gap with the United States.

  We recommend the White House National Security Council and the OSTP develop a more complete understanding of the state of play in each of these enabling technology areas, with the aim of identifying vulnerabilities and investment priorities. In addition, these bodies should integrate strategies and policies that promote and protect US AI-enabling technologies while punishing adversarial investments and theft in the critical national security technologies listed above. These efforts might be conjoined with the ongoing, multilateral International Telecommunications Union working groups on the topic.

Integration of Prioritized Technologies

In addition to prioritizing the technology and capability categories, whole-of-government direction should also extend to moving from development of novel AI technology to AI-enabled capability through AI investment and development supporting national security objectives. The US national security community can lack the sort of proactive and risk-tolerant approaches singled out in the DoD's strategy as being necessary to exploiting AI technologies, especially as it has sought to integrate new technology-enabled capabilities into its doctrine, organization, training, matériel, leadership, personnel, and facilities (collectively known as DOTML-PF).

Since the end of the Cold War, DoD has spent over $100 billion on systems that were eventually canceled, and expended countless more resources resulting from acquisition delays.[127] These can range from spending more than $5 billion on pixelated camouflage uniforms that actually made soldiers more visible,[128] to spending over $9 billion on WIN-T, a mobile intranet for Army brigades that is riddled with known cybervulnerabilities.[129]

Many of these canceled programs have integrated computer or information technology systems. A prime example: the family of networked air and ground vehicles collectively called the Future Combat System was canceled after more than $19 billion had been spent; then-Secretary of Defense Robert Gates decided in 2009 that the project would never be ready.[130]

Such challenges are not unique to the Unied States. China's PLA has a tendency to protect its own siloed research and acquisition programs known colloquially as "iron rice bowls."[131] Russia, meanwhile, has endured a series of failed acquisition programs due to mismanagement and cost overruns that have resulted in failed production lines including its fifth-generation air-superiority fighter, the Su-57.[132]

Still, the failures in integrating information technology systems will influence how the US national security community will approach integrating AI technology and could be one of several factors potentially eroding US advantage in military and security capabilities. As DoD laboratory and engineering research communities fund internal and external AI research that aligns with USG and DoD direction, tensions are likely to emerge between this funding and the acquisitions community, as well as the powerful congressional committees that determine military budgets. These latter stakeholders could have a more cautious perspective on the procurement and subsequent integration of technology that has yet to be fully proven.

Furthermore, it is unclear that the offices within the DoD and broader national security community that shape future R&D and acquisition priorities fully understand the scope of capabilities AI can enable. Nor has the national security community thought through how best to develop and deploy enterprise-wide education and training programs that will expedite adoption and use of AI-enabled capabilities across the US military and national security community.

To address this persistent integration challenge, the USG—led by DoD—should incorporate AI–enabled capabilities that are accompanied by formal and informal education and training programs *about the technology itself* and how it enables new capabilities for US national security. These programs can be managed by the military services within DoD and by appropriate entities within other government agencies and departments. They should include outreach to academia, the think tank community, and industry for speaker series, but more prominently to create curriculum that stresses both common issues associated with AI for national security and more agency-specific content to help relevant leaders and operators better understand how AI is applied in support of their specific mission.

The Future 'Data Gap' and Facilitation of Data Sharing

Reliable machine learning applications cannot be developed without an abundance of high-fidelity data. The more accurate and trustworthy data that AI engineers have access to and that algorithms can decipher and learn from, the more accurate and high-functioning the resultant algorithms will be.

Unfortunately, in this area the United States and many of its allies and partners may already be at a significant disadvantage to twenty-first century autocratic regimes because they control public data and use it for their own purposes.[133] The *Economist* estimated in July 2017 that China has over 700 million smart-phone users and assessed that "no other country could generate such volume of data to enable machine learned patterns."[134] China's leading high-tech company (and one of China's AI national champions), Tencent, claimed its WeChat messaging app had 963 million active monthly users at the end of the second quarter of 2017,[135] all of whom are providing data that can be exploited by Tencent to develop better algorithms and subsequently can be adapted and leveraged by the CCP regime.

Currently, ownership of data is experiencing a strategically significant shift. In China, this development is enabled and emboldened by legal, business, and political frameworks that prioritize regime security and national champion businesses over civil liberties and intellectual property rights. China's government is able to collect more personal data from the nation's citizenry, has access to all data collected through Western company joint ventures and other business activities in China, and makes Chinese businesses provide access to all data collected while doing business with more than one billion people.

According to February 2019 data from the International Data Corporation (IDC), China is accumulating an ever-larger share of the world's data, and is at least in the middle of a fifteen-year process of essentially switching places with the United States in terms of relative ownership of global data. In 2010, 27 percent of the world's data were stored in the United States, and 17 percent in China. By 2025, China is expected to have 28 percent of a global total of the world's data, which will be rapidly expanding due to widespread global digitization, while the United States will have only 18 percent; it is an almost exact reversal of positioning.[136]

The trading of places will be made even more strategically disruptive because of the magnitude of the total amount of data available in 2025 relative to 2010 or even today. IDC predicts that the global datasphere will grow from 33 zettabytes (ZB) in 2018 to 175 ZB by 2025. More than half of the world's data are still stored elsewhere, of course, but China's share of global data is growing 3 percent faster than the global average, according to the report. This offers opportunities for the Chinese government and Chinese companies to train more powerful models to support efforts to enhance state security, in particular (some of which will be exported outside of China), as well as national security. To be sure, the *type of data* collected does matter. Financial data will not necessarily enhance the quality of Chinese drone swarms. However, further refinement in the collection of voice, facial, and biometric data will be useful to the development of a range of military and security capabilities.[137]

Democracies, such as those in Europe and the United States, face an uphill battle to take similar advantage of data collected and stored in their own countries due to legitimate concerns over civil liberties and privacy. President Trump's executive order noted this challenge and established as an objective the need to "enhance access to high-quality and fully traceable Federal data, models, and computing resources to increase the value of such resources of AI R&D, while maintaining safety, security, privacy and confidentiality protections consistent with applicable laws and policies."[138]

The executive order should be commended for highlighting the importance of data and for minding, at least in theory, the need to balance AI urgency with legal, institutional, and constitutional protections. However, more detail on how the government shares its data with the private sector and applied-research centers is required as is an explanation of how data collected through the vibrant and pervasive US high-tech community can best be used to support broader USG and, more specifically, national security objectives. The present authors recommend the following steps to help guide the development of more open sharing of data both within government and between public and private sectors:

- **Create a Data Integration Task Force.** Integrating data from across the USG to support safe and more reliable AI development will necessitate the formation of a Data Integration Task Force designed to tackle myriad government datasets spread out across data silos, often in legacy systems and other cabinet-level agencies. This task force should be led by the chief data scientist, a position created by the previous administration that is currently unfilled. Only someone reporting directly to the president and with direct access to principal/deputy committee meetings has a chance at gaining the requisite data to apply against AI applications. Data cleaning must be paramount as high-quality data is an objective in and of itself and fundamental to safe and ethical AI. The Data Integration Task Force should be formed around a constellation of cross-cutting agencies such as the Defense Information Systems Agency (DISA), the Defense Digital Service (DDS), the Director of National Intelligence (DNI), and the Office of the Undersecretary of Defense for Research & Engineering (OUSD R&E). The task force should be tasked with collecting, cleansing, and aligning disparate datasets to ensure the data are fulsome and without error. Only then can the data be considered for AI.

- **Go beyond FEBP:** The Foundations for Evidence-Based Policymaking (FEBP) and OPEN Government Data Act are useful and welcome measures, but need to be followed up with more precise guidelines and frameworks ensuring not just data-sharing, but also data alignment—that is, that the data being shared contains coordinated development standards and metrics. New frameworks should extend beyond DoD and national security agencies. Establishment and implementation of data-sharing and acquisition protocols are one of the many areas of the AI development for national security strategy that the authors recommend and which require whole-of-government alignment across the agencies and offices referenced above. Such measures can offer more data to improve AI across the USG as well as facilitate adoption of the data standard that ensure multipurpose and multiagency use.

- **Adapt—not adopt—GDPR:** The EU's General Data Protection Regulation was implemented in 2018 in an effort to protect consumers and give them more control over the data they create online. It was also meant to simplify regulations, especially in Europe, to make transactions easier for businesses and consumers. The US Congress should consider GDPR as a template that can be adapted to harness the power and data exhaust of AI to both enable American enterprises as well as ensure its citizens are safe, not only from data they upload to the digital marketplace but also from data derived from private AI applications.

ENGAGE

"Engage" Summary and Recommendations

In order to better leverage the US world-class innovation system and high-tech community for national security, the authors recommend that the US national security community:

- Develop and deploy an effective strategic narrative to incentivize engagement
- AI applications for national security go well beyond kinetic capabilities
- "We are the good guys"
- Be a great—or at least better—customer
- Encourage engagement beyond Silicon Valley
- Enhance military-civilian fusion . . . with US characteristics
- Foster multistakeholder engagement

Narrative Building

The US high-tech industry and innovation ecosystem are among the country's most important assets—not to mention competitive advantages—in employing AI in support of US security and prosperity. However, to date, the US national security community has failed to fully engage this industry and ecosystem. Some observers see danger in this gap, one that Stanford University's Amy Zegart calls a "silent divide" between the two communities that is actively "weakening American national security."[139]

Recent discussion of USG engagement of the private sector has focused on tension between DoD and high-tech companies. An internal Pentagon memo that *Wired* reported had circulated to roughly fifty defense officials in June 2018 underscored the importance of remedying this divide. According to the article, which was produced in partnership with the Center for Public Integrity, the memo says the United States "will not compete effectively against our adversaries if we do not win the 'hearts and minds' of the key supporters"[140] in the US high-tech community.

High-tech community resistance to working with the national security community is multilayered. The pressure applied by thousands of Google engineers to abandon Project Maven over the perception that helping DoD more accurately identify possible targets violates Google's "don't be evil" mantra is just one particularly emotionally charged argument against collaboration. Engineers at Microsoft expressed a similar concern after the company was contracted to deliver customized HoloTech virtual and augmented reality headsets to the Army to support training and "increased lethality." Microsoft, however, did not abandon the $470 million deal, suggesting that ethical concerns will not derail national security and defense projects at all high-tech companies.[141]

A more common concern is practical in nature: doing business with the government is difficult. It involves a ponderous acquisition system and regulations, especially around intellectual property retention and profit margins, that disincentivize involvement. Companies across the ideological spectrum have one consistent request: "don't waste my time."

This disconnect does not have to persist, and there may be more common ground to be explored between the national security community and the high-tech sector than is revealed by current objections and frustrations. Finding and taking advantage of that common ground requires crafting of a nuanced, but direct and compelling narrative that allows America's global-leading AI industry to identify and engage in opportunities that align with their values and priorities. It also will require the USG and DoD, in particular, to adapt or fundamentally revamp processes, expand engagement, and generate interagency collaboration associated with AI development. The United States should consider establishing global, not just national, narratives and risks that enable not only US-based AI technology companies to engage with the US government but also leaders in AI located outside the United States.

- **Strategic narrative development.** The June 2018 internal Pentagon memo, as reported in *Wired*, underscored the importance of narratives and the damage done to USG engagement with the US high-tech industry and, in particular, DoD "stumbling unprepared into a contest over the strategic narrative."[142]

  Developing a layered narrative that offers justification for and flexibility to high-tech engagement with the US national security community is a foundational first step. This narrative should revolve around a set of key themes highlighted throughout this paper and should be nuanced enough to speak to companies across the spectrum of support for DoD and national security community AI development: from objection or ambivalence to support. There are several foundational elements:

  Communicating the changing nature of conflict and expanding opportunities for engagement. The fusing of states of peace and war, of the physical and digital worlds, and of reality and perception have expanded national security threats and competitions well beyond the kinetic or traditional defense missions. Deepfakes, smart bots, and AI-enabled manipulation of social media are also of concern to the high-tech industry, eroding trust in platforms and threatening the viability of their business models.

Supporting national security, then, does not have to mean supporting any phase of the deployment of weapons or "increased lethality." Demand for development of AI in support of objectives such as enhancing personnel safety and improving logistics is increasing, as is demand for devising means of deterring, dissuading, detecting, and defeating cyberattacks and other AI-infused efforts to undermine the stability and efficacy of the US polity and society. Google is to be commended in this regard for its ongoing effort to work with DoD to help identify deepfakes, which are already doing damage to the security and stability of the United States.

Being the "White Hats." The United States are "the good guys," as General Joe Dunford, then-chairman of the Joint Chiefs of Staff, was quoted as saying during the Halifax Security Forum in November 2018.[143] Moreover, the institutions shaping and implementing US national security and defense strategy are parts of a democratic system, and are there to, as Microsoft CEO Satya Nadella is quoted as saying by CNN Business, "protect the freedoms that we enjoy." Engaging with institutions—and potentially helping to shape not just the technologies being developed, but also how they are employed—is, again according to Nadella, "a principled decision."[144]

The white hat argument gains more credence when placed in the broader context of the competition between liberal democracies, including those in which institutions and norms are under considerable duress, and authoritarianism. China's use of and efforts to export AI technologies to collect biometric data and reinforce dystopian authoritarian control over populations stands in stark contrast to the measures (if frequently responsive rather than proactive) U.S federal, state, and local government have taken to balance constitutional protections and comfort of use concerns with technology and capability development. San Francisco's city council decision banning use of facial recognition software by city agencies or the police (but not private businesses) exhibits an inherent anxiety about potential government misuse of advancing technologies not resident in China or Russia.[145] So, too, does the rerelease of the 2019 request for information related to the Army's ATLAS autonomous vehicle program, which underscored human control of the system.[146]

Examples of misuse of AI or efforts to stretch the boundary of ethical use do exist in the United States: Chicago and New Orleans police departments using AI-enabled "predictive policing" methods qualify as at least approaching the boundaries of ethical use and worthy of review.[147] And only the naïve would suggest that future iterations of these types of programs are no longer being pursued or that the US system is impervious to pressures to use cutting-edge technology to enhance security. Vigilance will be in constant demand to ensure safe and accountable use of AI.

However, strong responses to these programs reflect at the least a feedback mechanism that can alter or limit widespread implementation of controversial AI applications over time. US legal institutions play a powerful role in ensuring not just responsible AI but also "accountable AI"; in other words, leveraging the Department of Justice and Department of Defense together to fund R&D into further "Explainable AI" programming and putting in place codified legal safeguards that ensure the irresponsible or unethical employment of AI is held to account.

This context is necessary in part because many leading US high-tech companies are already collaborating with Chinese universities and commercial entities on AI programs. Amazon and Microsoft announced plans to open new AI research labs in Shanghai on September 17, 2018, at the state-backed World Artificial Intelligence Conference in Shanghai. Google was another prominent participant at the event. Google opened an AI center in Beijing in December 2017.[148]

This collaboration may have no seemingly direct connection to the sorts of technologies being deployed to repress Uighur Muslims or surveil citizens, and is the result of a relatable capitalist instinct to capture more share of a promising market that requires collaboration with local entities. Of course, such cooperation has implications well beyond building earnings calls and the development of better electronic widgets for Chinese citizens. The effects of these partnerships radiate well beyond the commercial sector and have proximate effects for US national security.

China's policy of military-civilian fusion is a long-standing initiative that China's leadership has repeatedly emphasized in public statements and documents over the last half of a decade as being a key mechanism through which China can leverage technology developed in or acquired from commercial relationships for military purposes. During the first meeting of the Central Commission for Integrated Military-Civilian Development—chaired by President Xi himself—held in June 2017, Xi laid a list of military-civilian fusion priorities including "advanced weapons and defense equipment, science and technologies, maritime, space, cyber defense, and alternative energy."[149] Supercomputers, AI, information networks, and enhanced autonomy for unmanned systems were subsequently identified as more specific priorities.[150]

Articulating risks. The issue of US high-tech AI collaboration with China reached a boiling point in March 2019 when General Dunford publicly criticized Google for the apparent contradiction of its Project Maven decision while still collaborating with Chinese entities on AI projects that will, through military-civilian fusion, be utilized by the PLA or to enhance surveillance capabilities.[151] Google has agreed to discuss these concerns later in 2019.

Many businesses outside the US defense and security industry lack a full understanding of the nature of the military-technological competition between the United States and China and the national security implications of China's technology acquisition. These companies, understandably, are far more prone to seeing the purported opportunity of China's market—whether it is the high-tech/ICT industry, commercial aerospace, or other industries. Samm Sacks, a senior fellow at the Center for Strategic and International Studies, estimated that China accounted for $23 billion of US information and communication technology exports in 2017.[152] It is not reasonable to assume that US companies will simply abandon the potential for revenues and shareholder earnings that comes with doing business in China, absent a fundamental—and potentially disastrous—decoupling of the US and Chinese economies.

But these companies can make better, more informed decisions about the risks—both to their intellectual property and to US national security that comes with engagement in China's market. And here, the USG has an important role to play in helping establish a common understanding of the nature of China's technology acquisition challenge and the importance and dimensions of the US-China AI, 5G, semiconductor, and overall military-technological competition. Key focus areas of this effort could include identification of technologies and research areas most in demand by China's military and security communities, the scale and methods of the technology-acquisition program, and the overall risks and challenges associated with doing business in China.[153]

Process, Regulation, and Mindset

Beyond narrative-building, the USG should take specific, focused actions to encourage and optimize engagement with the high-tech community.

- **Be a better customer through procurement and data-sharing.** The USG should take at least two proactive steps to reduce the friction associated with doing business with the public sector.

  First, the process for procuring commercial-off-the-shelf information technologies should be reformed to ensure shorter business development and acquisition cycles. As part of this process, the present authors recommend pooling procurement data, as well as optimizing data metrics associated with talent development, both of which will enhance the engagement with the US high-tech community. By applying AI to process petabytes of data on how the government buys services and equipment, Washington has the potential to offer everyone from Microsoft to the nascent start-up in a WeWork office something of immense value: a great customer!

  Second, adoption of data-sharing agreements will allow the government to loosen constraints on data sharing and make the internal technology environment more friendly to commercial AI start-ups offering solutions. Workable data-sharing agreements will address the distinct concerns of each side, although a primary concern for government stakeholders is access to data.

  Parameters must be set on who has access to data and how data will be handled, and then bound by statutory, legal, or administrative constraints. In order to address technology partner concerns about maintaining independence with the use and interpretation of data, there are common elements in data-sharing agreements:[154]

- authorizations and protocols for those handling data
- limitations on the use of data
- "no surprises" clauses that ensure the agency's right to review findings before they go public
- a plan for data security
- ownership of data
- conflict-resolution procedures
- modification and termination of services

- **Engage beyond Silicon Valley.** The academy is another underexploited US advantage. There are certainly instances of applied research emanating from the leading global universities in the United States including, for example, GTRI's Angry Kitten cognitive EW program discussed above. However, more can be done to transition the basic research being carried out in US universities to move toward applied research and also to protect the strategic technologies they develop.

  The US and state governments should intensify engagement with the technology transfer offices resident in most universities, incentivizing universities to establish and maintain strong offices through research grants and public-private partnerships directed at ensuring their health. Universities can offer internships and fellowships, potentially supported by government or corporate partnerships. This will take some time as most universities excel at basic research. Shifting their focus to applied research should be enabled through government partnerships, much like what the Department of Defense has done with its University Applied Research Center (UARC) initiative.

- **Enhance military-civilian fusion . . . with American characteristics.** The Chinese adoption of military-civilian fusion is well-documented and has shown increasingly material results, especially over the last five to ten years. Since Xi Jinping ascended to power in 2012, civil-military fusion has been part of nearly every major strategic initiative, including the 2015 Military Strategy White Paper, Made in China 2025, and Next Generation Artificial Intelligence Plan.[155]

  The goal is to bolster the country's innovation system for dual-use technologies through "integrated development." In the military, the recently established Strategic Support Force has signed cooperation agreements with research universities. A number of municipalities and provinces, like Tianjin, Shanghai, Shanxi, and Guangdong, have joined the effort, promoting the development of local industrial clusters that could allow large defense enterprises to work with research institutes and private companies.

  The United States should assess this progress and consider expanding as well as improving existing initiatives like the Defense Innovation Unit (DIU) that could serve as pillars and conduits of military-civilian fusion, with American characteristics. Originally conceived as DoD's outpost in Silicon Valley to scout and engage with the high-tech sector, DIU efforts to date have largely emphasized accelerating the speed of contracting. Supporting and expanding fast-track mechanisms such as other transaction authorities (OTAs) that enable procurement of commercial off-the-shelf (COTS) technology from vendors of choice remain priorities. But these programs, while helpful, are only the tip of the iceberg when considering how best to accommodate industry expectations regarding retaining intellectual property rights for key technologies and enabling government to quickly fund and programmatically enable the consideration and purchase of COTS software.

The United States should also leverage relationships with commercial entities that decentralize its innovation ecosystem by encouraging freethinkers and problem solvers to address and work through tactical and systemic problems, rather than relying on the bureaucracy to eventually resolve them. The government can start by working with commercial accelerators like Techstars, which already has a successful relationship with the US Air Force to train commercial-government mentors who can support the successful integration of tech start-ups into the government ecosystem.

- **Foster multistakeholder engagement.** AI strategies work only if there's a broad consensus from all stakeholders, meaning that the discussion of engagement of the US high-tech community in support of US national security, societal and political stability, and prosperity should be broadened well beyond a focus on DoD activities to include federal and state agencies. Synchronization of public- and private-sector priorities, objectives, and, critically, programs is crucial, but so, too, is the alignment of the Departments of Defense, State, Energy, Education, and Transportation, and assorted local and state institutions.

GOVERN

"Governance" Summary and Recommendations

AI research has reached sufficient scale and effectiveness within the defense and security space to warrant a better understanding of the dimensions of both the immediate and longer-term ethical and safety risks. Risks associated with the use of biased or incomplete data, as well as malicious corruption of data, present special challenges.

The United States has an obligation to create national standards and norms around ethics and safety. It also has an opportunity to take the lead in shaping these norms at an international level as a means of slowing applications of AI that threaten US security, political and social stability, and values, such as AI-enabled domestic surveillance, lethal autonomous weapons systems, and adversarial examples.

Key recommendations include

- Increase funding for research on AI safety
- Develop and demonstrate national standards for ethical and safe AI that can, in conjunction with other states, serve as a framework for global norms that protect individual privacy, freedom, liberal democratic values, and human rights
- Create mechanisms for accountability of AI development and implementation
- Leverage institutional influence to shape norm- and standard-setting

Ethics and Safety

Innovation in AI is outpacing the capacity of government, defense, security, and private-sector stakeholders to keep up with many of the adjacent innovations required to ensure effective transition from technology development to the deployment of a new capability.

This is especially the case for the ethics and potential regulation of AI. Capabilities under development such as LAWS, AI-enabled domestic surveillance, and AI-enabled human performance enhancement raise sometimes tricky ethical questions around which there is unlikely to be unanimity of opinion within the United States, between it and its allies, or in the international community.

Consensus about the risks of "killer robots" generally and the undesirability of the worst-case scenario of these robots operating outside, contrary to, or beyond human expectations can be easily reached.

The problem of having AI act outside of human intention escalates as AI becomes more intelligent. Oxford Professor Nick Bostrom devised a thought experiment in 2003 that stresses the problem of a superintelligent machine being given the goal of maximizing paper clip production, ultimately destroying the world in its pursuit of making more paper clips.[156] He raises risks associated with a machine's pursuit of its objective—even one so seemingly trivial as paper clip production—that can lead it to act outside of original human intent with potentially disastrous consequences.

How best to manage this acute, potentially existential, challenge generates a range of responses. Eric Schmidt, the former CEO of Google, has suggested a relatively simple solution—one familiar to any technological Luddite with a frozen computer screen—for dealing with lethal autonomous weapons systems operating beyond the original parameters of their algorithms: "We would unplug Terminator if it showed up . . . Were the killer robots to start, we would find a way to stop them."[157] Researchers at Alphabet's DeepMind announced in 2016 that the company has developed a "big red button" that will stop runaway artificial intelligence and keep it from causing harm.[158] Such assurances are unlikely to offer much comfort to those who seek to ban research and development on lethal autonomous systems altogether.

Killer robots are probably the bluntest and bleakest example of ethically questionable applications of AI. Deployment of these systems is not imminent yet. Discussion of the ethics and safety of these systems is warranted and indeed, can inform more nuanced ethical debates about other AI-enabled capabilities.

Consider the AI border guard and Taylor Swift stalker detection versus China's use of AI to repress Uighur Muslims and establish near complete social control over 1.4 billion people: These examples are indicative of the ways in which the issue of "good" and "bad" uses of AI will test US national security. Can the United States pursue its foreign, national, and security policy objectives in a world in which China is exporting the tools of authoritarian control to more and more states around the world? If not, what recourse does the United States and its allies have to shape a world in which such AI applications are constrained?

Data Integrity and Privacy

To these important questions should be added concerns about data integrity and privacy, deepfakes, adversarial examples, algorithm bias against underrepresented groups, and testing to ensure that AI not only works the way it was designed, but also that it operates fairly and does not favor one group or outcome or condition more than others. Data are core to AI development, but large amounts of poor or intentionally corrupted data will further the development of unsafe and counterproductive AI applications.

The development of AI is at a relatively early stage. It will improve and applications will expand, both in the defense and security space and elsewhere. Even if one believes that the most profound risks to humanity presented by AI are half a century away, there is still an urgency to better dealing with the short-term risks of the novel, immature, but still affecting and powerful, technologies that are available today (or nearly so). There also is a similarly urgent need to begin to both understand and mitigate against the risks that could consume AI development in the decades ahead.

Unfortunately, the complexity of the discussions of ethical AI has deterred research on the topic. A December 2018 report on global AI research from global information analytics company Elsevier reveals that "the ethics of AI are a blind spot."[159]

Some organizations and countries are making first attempts to raise the issue of safe and ethical AI. The EU released its ethical guidelines for trustworthy AI in April 2019.[160] These parameters underscore the importance of AI that is:

- lawful, respecting all applicable laws and regulations;
- ethical, respecting ethical principles and values; and
- robust, both from a technical perspective while taking into account its social environment.[161]

The EU framework also stresses concepts such as human agency and oversight, full control of data by citizens, transparency, nondiscrimination and fairness, social and environmental well-being, and accountability. These are all good places to start.

France and Canada have contributed to the debate over ethical AI. The two US allies established the International Panel on Artificial Intelligence in December 2018 to shape the discussion of "responsible adoption of AI that is human-centric and grounded in human rights, inclusion, diversity, innovation, and economic growth."[162]

Significantly—and somewhat ironically—China is taking at least superficial steps to demonstrate its concern about AI safety and ethics. In January 2019, the Chinese Association for Artificial Intelligence appointed Chen Xiaoping, a leading AI scientist in China and inventor of the "realistic robot Goddess" Jia Jia and "intelligence home service robot" KeKia, to lead an AI ethics committee.[163] Chen spoke of the current and imminent risks of AI noting that "if the technology was far off being applied there would be no need to talk about ethics research, but there is value in this research into technologies that might be applied on a large scale in the next 10 or 20 years."[164]

The United States should welcome the deepening and broadening engagement in AI safety and ethics/trustworthy AI. This opportunity can reinforce the United States' status as the global leader in shaping relevant norms in international relations and security, and as a means to gain advantage in the AI development and geostrategic competition with China.

- **Fund AI safety research.** The United States should increase and direct funding for research on ethical and safe AI, with a particular focus on AI ethics for the defense and security context. Machine learning is difficult to track, assess, and monitor by design, but further research through National Science Foundation grants to universities and research institutes among others could enable humans to accurately assess whether an AI application and its intended employment will compromise rather than reinforce safety, stability, or security of individuals, populations, and political, economic, and social systems.

  This research support should include substantial funding for programs mentioned earlier in the report such as DARPA's "Explainable AI" program.

- **Become a global leader in the development of global AI standards.** This opportunity focuses on standards, not norms, and should be pursued through whole-of-government demonstration of ethical and safe development of AI as well as increased investment in technical and strategic research into the safe and ethical use of AI. It also can be achieved by focusing on an initiative the DoD has made a priority: advocating for a global set of military AI guidelines that incorporates engaging the "broadest-possible audience."

  Effective global regulation of military capability is a difficult task. It requires the alignment of perspectives of actors with varying viewpoints on the utility, safety, and ethics of specific military capabilities and also limits the means through which nations pursue their own security, stability, and prosperity. The strategic context of a world in transition and characterized by intensifying geopolitical competition and loosening alignments further complicates the task. However, there are some historic markers that suggest regulation of military capabilities and—more relevant to the discussion of AI in defense and security—*applications* of these capabilities is possible, even in the context of intense competition.

The ban on chemical weapons after World War I and agreements on the size and composition of nuclear arsenals are useful, if inexact, examples. These were expensive victories borne of real-world examples of the grotesque human suffering use of these weapons would—not could—inflict. A better and more constrained model for a preemptive AI arms agreement is found in the uneasy, and currently fraying, Outer Space Treaty prohibiting the weaponization of space.165 Established in 1967—at a period in the development of space technology that is *roughly* analogous to current development of AI—the treaty has not stopped the *militarization* of space infrastructure, but it has for over fifty years prevented the weaponization of or a meaningful conflict in space. States have developed and tested, but, critically, not fully deployed or used in anger capabilities that would put the treaty's efficacy in question.

This may well be the best result for the future of AI regulation in the short term: a clear-eyed deal that regulates but may not completely ban the application of the use of AI as part of specific applications, or in certain domains, and that can be built on as military and dual-use applications of the technology develop. It is a result that will only be achieved with USG leadership.

- **Leverage institutional influence.** Lastly, since AI technology does not stop at the waters' edge, the administration should consider engaging multilateral bodies like the Group of 20, as well as G20 members that are major players in the sector such as South Korea, China, Germany, and Japan, to establish standards for government datasets that can be shared for private research, data transparency, AI accountability, and a legal framework for evaluating what constitutes infringement of a citizen's rights.

COMPETE

"Compete" Summary and Recommendations

All decisions taken, priorities decided, or funding dedicated to AI development supporting US national security will be viewed through the prism of US-China geopolitical and AI/high-tech competition. Indeed, recommendations included in the direct, engage, govern, and protect components of our proposed strategy are designed at least in part to help better position the United States in this competition.

This competition centers on the United States and China, but it involves US allies and private-sector companies, all of which are playing important roles in how it evolves. Think of US efforts to convince allies in both the Indo-Pacific and Europe to forego doing business with Huawei or the AI and high-tech relationships China's state-owned enterprises, high-tech community, and academic institutions have formed with US allies. Sustaining advantage in it is a crucial component of AI development for national security—and of our proposed strategy. Some measures the United States should take to meet this competitive challenge include:

- Engage allies
- Understand allied innovation systems and AI ecosystems
- Develop competitive strategies
- Focus on war-gaming and red teaming
- Incentivize talent development, recruitment, and retention

Competitive Strategies

The US-China AI development competition is frequently referred to as an "AI arms race," a label that many have rejected as inaccurate; AI is not a weapon, and deterministic frequent references to an AI arms race will only serve to make it so.

Nonetheless, the term is useful in conveying the urgency and the intensity of the competition facing the United States regarding the development of a technology area that is likely to disrupt global economics, geopolitics, and, yes, military and security capabilities across at least the eight categories identified in this paper. Russian President Putin articulated the stakes of the global AI competition when he stated, "Whoever becomes the leader in [AI] will become the ruler of the world."[166]

This competition is at an inflection point where continued US leadership in core technologies is being challenged both by China's increasing innovation capacity and by the changing nature of the AI competition itself. The advantages buttressing US global leadership in AI core technologies—technological proficiency and innovation capacity—may become less relevant as core AI *technologies* diffuse widely and the main competitive axis becomes development and deployment of new *applications.*

According to Kai Fu Lee, the former head of Google China who currently leads a Chinese high-tech venture capital firm, Sinovation Ventures, and is a practitioner in both the Chinese and US AI ecosystems, China's "speed, execution, product focus, access to data, and government support are significantly higher than their American counterparts."[167] Lee also notes that these are the attributes that will be most in demand in the future AI development competition.

Of course, Chinese leadership in AI is far from certain—alarmism in this area is nearly as counterproductive as dismissiveness—but the current balance in assets to be exploited *is* shifting and not necessarily to the advantage of the United States. As Frederick Kempe, president and CEO of the Atlantic Council, noted upon his return from the World Economic Forum in January 2019:

> *Most troubling for the American business leaders in Davos, who had grown accustomed to being atop the global technological heap, was that they heard time and again how quickly they were falling behind their Chinese peers. Though it is a technology race most Western executives feel is only on its first laps, they heard how President Xi had declared a sort of space race or Manhattan Project around AI that is already delivering measurable results.*[168]

Meeting this competitive challenge requires a combination of constructive engagement of allies and filling gaps in USG knowledge about important components of the US-China competition.

- **Engage and manage allies.** The United States is not effectively leveraging one of its greatest assets: its allies. The United States' over thirty formal treaty allies in Europe and Asia provide a deep pool of data and technology resources, but legal restrictions have prevented greater coordination and even joint development. By way of example, European privacy laws hinder the data sharing necessary for AI development. For many in Silicon Valley, it is more burdensome to collaborate on AI with governments and firms in Europe than in China. Yet, the fact that AI algorithms depend on data mean that no nation, including China, has an a *priori* advantage. This makes data sharing among the United States and its allies all the more paramount.

  The United States should lead a new grouping of the world's leading democracies, including European and Asian allies, initially to consult and coordinate annually on technology policies, leading eventually to a standing technology alliance similar to the National Technology and Industrial Base.[169] This legal agreement between the United States, UK, and Australia aims to reduce barriers and create frameworks for effectively integrating technology in mutually supportive capabilities.

  The "Five Eyes" intelligence pact, involving the United States, UK, Australia, Canada, and New Zealand, needs new operating guidelines for focusing on the competitive dynamic with China and especially with its AI development. While different states may see China's AI development with varying degrees of concern—and, indeed, some states are supporting joint research with Chinese entities in this area—this core group of allies could offer a strong starting point for multilateral efforts to mitigate risk associated with China's AI development.

  Other areas of possible collaboration include:

  - joint development programs, for example in unmanned systems such as the low-cost attritable unmanned combat aerial vehicle program sponsored by the Australian Department of Defence, but overlapping with US research on the loyal wingman concept;[170]
  - data-sharing standards; and
  - defense and security interoperability standards, to ensure development of AI capabilities that will be deployed both by and to support key allies.

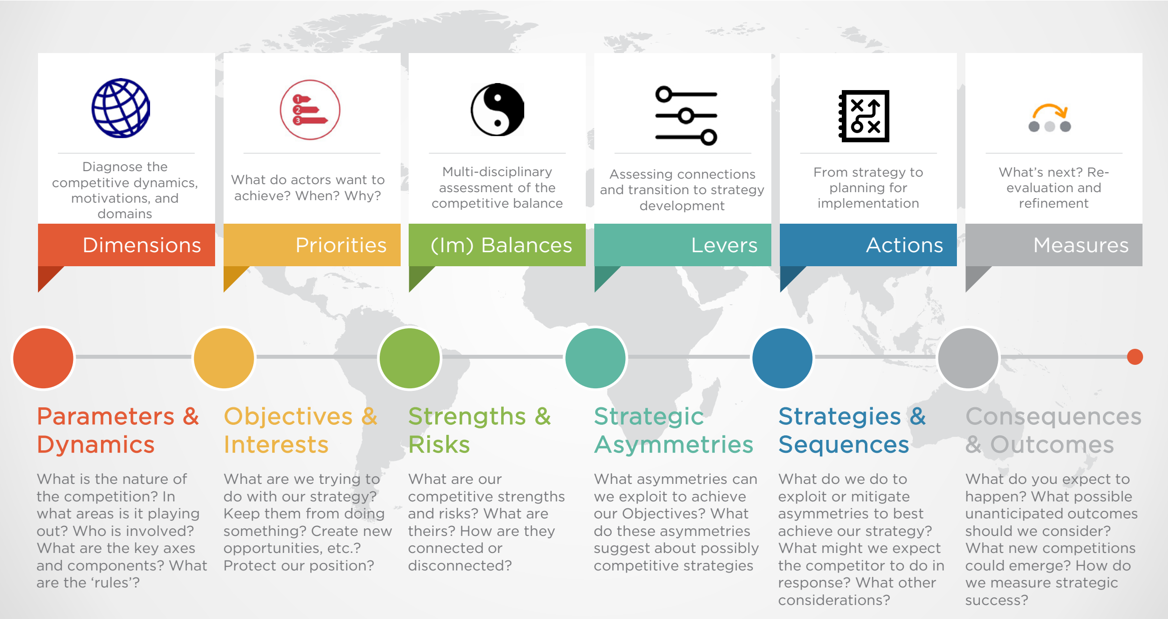
The mechanism for driving this engagement should be through a combination of bilateral and multilateral agreements around AI that expand upon existing intellectual property norms and legal frameworks. These agreements should allow for sufficient sharing of information and data between countries, not unlike the economic treaty between France and Germany that includes AI technology codevelopment.[171] It also should include some engagement with multilateral institutions, as difficult as working with these institutions can be. As was stated in the pages of the Atlantic Council's Global Innovation Sweepstakes publication, multilateral institutions such as the

World Intellectual Property Organization should play a crucial role via the administration of the Patent Corporation Treaty, the collection and rigorous analysis of global intellectual property data, and implementation of programs to strengthen national intellectual property rights (IPR) systems.[172]

- **Assess and map allied capabilities.** The USG would benefit from a more detailed and integrated understanding across the national security enterprise of the capabilities that its allies possess. Specifically, interagency sharing of allied AI-enabled innovation systems and capabilities should be aligned with funded research in order to optimize:
  - key components of allied and partner innovation systems;
  - AI innovation capabilities;
  - AI research and development priorities; and
  - key relationships with the United States, China, and other states.

- **Develop military-technological competition net assessment and competitive strategies.** An effective, whole-of-government US strategy for maintaining AI advantage should include a comprehensive net assessment of the military-technological competition and, specifically, a focused assessment of the AI competition between the United States and China.

  Useful research on the dimensions and dynamics of this competition has already been completed and is available in open and publically available sources. However, considerable room still exists to expound upon this analysis and, critically, to tie the relative strengths and weakness of China and the United States into broader competitive strategies; that is, strategies that identify and exploit asymmetries and drive competitive dynamics into directions in which the United States is likely to maintain advantage.



Diagnose the competitive dynamics, motivations, and domains

Dimensions

Parameters & Dynamics

What is the nature of the competition? In what areas is it playing out? Who is involved? What are the key axes and components? What are the 'rules'?

What do actors want to achieve? When? Why?

Priorities

Objectives & Interests

What are we trying to do with our strategy? Keep them from doing something? Create new opportunities, etc.? Protect our position?

Multi-disciplinary assessment of the competitive balance

(Im) Balances

Strengths & Risks

What are our competitive strengths and risks? What are theirs? How are they connected or disconnected?

Assessing connections and transition to strategy development

Levers

Strategic Asymmetries

What asymmetries can we exploit to achieve our Objectives? What do these asymmetries suggest about possibly competitive strategies

From strategy to planning for implementation

Actions

Strategies & Sequences

What do we do to exploit or mitigate asymmetries to best achieve our strategy? What might we expect the competitor to do in response? What other considerations?

What's next? Re-evaluation and refinement

Measures

Consequences & Outcomes

What do you expect to happen? What possible unanticipated outcomes should we consider? What new competitions could emerge? How do we measure strategic success?

Figure 6: A process for developing and refining competitive strategies.

SOURCE: TATE NURKIN

- **Focus on war-gaming, red teaming, and scenario planning.** The US-China military-technological and AI-focused competition is iterative and dynamic. Employment of red teaming methods designed to better understand competitor and adversary mentalities and tools such as war-gaming and scenario planning will be particularly useful in capturing these iterative and frequently difficult to predict behaviors and dynamics. Incorporating these strategy support tools can help the United States hedge against how China's AI strategy and response to US actions and decisions might drive new competitions or asymmetries.

  The United States can and should invest heavily in the incorporation of AI tools into war-games and simulations. The US has a strong history of leveraging war-gaming, modeling, and simulation to support revolutionary changes in military affairs and assessing the strategic, operational, and tactical effects of disruptive capabilities. In the case of AI-enabled simulations, DoD in particular should work through DARPA and DIU to take advantage of the full scope of commercial AI-enabled simulations and gaming as they relate to modern military capabilities. This work includes assessing commercial algorithms that might readily be incorporated into existing DoD products like the US Army Game Studio's *America's Army,* which integrates factors such as courage and teamwork, and more advanced products such as *Virtual Battlespace 3.,* produced by Bohemian Interactive Simulations.[173]

  DoD should also work through the Office of the Secretary of Defense and each services' strategic studies group to assess how they can incentivize commercial industry to develop simulation and war-game capabilities that accurately predict human behavior in a model, like the OpenAI Project is doing with Dota 2.[174] These same groups should study the cultural reasons why it has been difficult in the past to implement an AI-enabled model that may not necessarily do what a general or admiral wishes, much the same as what Lieutenant General (ret.) Paul van Riper famously demonstrated in 2002.[175]

The Competition for Talent

Talent development, recruitment, and retention is a crucial axis in the US-China AI competition and a vulnerability for many other countries' efforts to scale AI development.

As demand for new AI applications in the defense and security space and beyond grows, supply of coders and AI engineers will need to expand rapidly to keep pace. So far, the supply has lagged behind demand at a global level and in the United States and China.

Chinese high-tech giant Tencent produced a 2017 *AI Talent White Paper* that assessed there are only 300,000 AI researchers and practitioners worldwide, a shortage of more than ten times the expected demand.[176] The paper also found that there were fewer than a thousand people at the very highest level of AI talent capable of steering the direction of AI research and development globally. The US has approximately 46 percent of the available pool of talent, and maintains a lead in advanced AI research within universities compared with China's nascent academic research.

The *Global Times,* frequently a mouthpiece for the CCP, published an article in January 2018 that decried that "the world's second largest economy had not gone far enough in building its AI talent reservoir to match its ambition to lead global AI development."[177] The article cited the Tencent report as well as a July 2017 LinkedIn survey that ranked China seventh in volume of AI professionals with only fifty thousand. According to LinkedIn, the United States had 850,000 individuals on its platform listing involvement in AI. Of course, the measure of AI professionals self-identifying as such on LinkedIn is more directional than scientific, but its findings are roughly equivalent with Tencent's and with other research on the topic.

China's Next Generation Artificial Intelligence Development Plan lists talent development and training as a key metric and objective across each of the three phases of the plan, which culminates with China being a global leader in training and recruitment by 2030. Other national AI strategies have been focused largely or even solely on talent or recruitment to a degree that talent and skills development are listed as one of eight pervasive priorities across the eighteen national or regional AI strategy plans published to date. Canada and South Korea's plans are predominantly focused on funding talent development.[178]

As a result, China is pursuing several measures to build depth and gain advantage in human capital focused on key science and technology areas. According to the US-China Economic and Security Review Commission:

> *[The] Chinese government maintains government programs aimed at recruiting overseas Chinese and foreign experts and entrepreneurs in strategic sectors to teach and work in China. Moreover, Beijing utilizes intergovernmental and academic partnerships and collaborations in the United States, establishes Chinese research facilities in the United States, and sends experts abroad to gain access to cutting-edge research and equipment without disclosing the organization's or individual's connections to the Chinese government.*[179]

In addition, the top-down guidance of the Next Generation Artificial Intelligence Plan has incentivized local governments to generate their own talent recruitment initiatives. In Shenzhen, the local government provides incentives for individuals to live in the city in order to attract talent. One such program has reportedly attracted in excess of 1,200 individuals including the founders of Intelli-Fusion, which has developed advanced applications in facial recognition.[180]

But the diagnosis of an overall shortage in AI talent that affects China and the United States as well only tells part of the story. China is actively working, in a way that is more difficult for the United States to do, to focus some of its most promising young high-tech minds on military applications of AI.

In the fall of 2018, the Beijing Institute of Technology announced it had selected thirty one "patriotic" seventeen- and eighteen-year-old students—out of five-thousand applicants—to join a program explicitly designed to teach young technical minds how to weaponize AI. Students in the program are mentored by an academic in the AI field as well as a member of China's defense industrial base.[181] When combined with other measures designed to recruit Western-educated AI academics and scientists back to China (or to collect on China's behalf), these measures create the picture of a country committed to building human capital to deliver a competitive advantage not just in AI development, but in AI-enabled defense and security capabilities.

- **Talent development and retention.** Both the DoD strategy and the executive order address this challenge. DoD's strategy calls for "cultivating a leading AI workforce,"[182] which involves adapting DoD culture, skills, and approaches.

  This is more easily said than done. The USG's current culture and operating practice in hiring new talent is frequently unwieldy and time-consuming. It can take several months (at a minimum) to hire qualified candidates, and the pay is significantly less than equivalent jobs in the private sector. A relevant data point: The New York Times reported in October 2017 that "typical AI specialists, including both PhDs fresh out of school and people with less education and just a few years of experience, can be paid from $300,000 to $500,000 a year or more in salary and company stock in order to cope with this potential constraint."[183]

  DoD officials and the wider national security community know they cannot compete with these private-sector salaries. The answer is to continue to rely on contractors (including federally funded research and development centers) as well as its university affiliated research centers and the broader academic community, which may affect DoD's objective of encouraging "rapid experimentation, and an iterative, risk-informed approach to implementation."[184]

  The USG can begin to address this shortfall by offering a noble mission to the private-sector workforce, rather than framing the relationship with the private sector in terms of pure financial gain. The opportunity to serve and support the country is real and has resonated throughout time.[185] By recruiting outstanding commercial talent for specific missions, similar to what the Defense Digital Service has done, the USG can leverage commercial talent against system-wide problems like data-sharing agreements, data integration, or legal structures to ensure AI accountability.

- **Expand beyond STEM-C.** Much of the focus of skills development for all countries is justifiably on science, technology, engineering, mathematics, and coding (STEM-C). Successfully navigating the AI innovation process all the way to deployment of a valuable capability, however, requires more than technical skill. Also necessary are:

  - management skill sets to ensure AI development efforts are coordinated and dedicated on articulated priorities;
  - strategic thinking to prepare for effects—anticipated and otherwise—of AI development and iterative and dynamic competition;
  - creative operational thinkers required to devise effective operational concepts and understand how adversaries and competitors might deploy AI to affect US national security;
  - marketing and communications personnel to devise and implement strategic narratives; and
  - legal and regulatory acumen.

PROTECT

Meeting the Theft and Acquisition Challenge

In a speech to the Council on Foreign Relations in April 2019, FBI Director Christopher Wray made a clear and definitive statement about the threat to US national and economic security stemming from economic espionage and technology theft. According to Wray:

> *Economic espionage dominates our counterintelligence program today. More than ever, adversaries target our nation's assets, our information and ideas, our innovation, our research and development, our technology. And no country poses a broader, more severe intelligence collection threat than China.*[186]

"Protect" Summary and Recommendations

China's ongoing proactive and aggressive technology-acquisition program is of acute concern to the United States. New means of protecting US technology from either illicit/surreptitious or licit transfer of US AI technology is a crucial part of the US AI development approach.

Key recommendations include:

- Enlist support
- Enhance IP protection
- Safeguard patriotic investors

Worry over China's technology theft is, of course, not confined to the FBI or Department of Justice. It is a growing widespread concern across the US national security community, including within DoD, where the theft of military technologies has led to several familiar-looking weapons systems within the PLA arsenal—from unmanned systems to stealth fighters and beyond. China's purported hacking of a US Navy contractor and theft of sensitive data on US missile and undersea programs in June 2018 is another in a long list of identifiable instances of China using the vulnerabilities of the information domain to undermine US national and economic security.[187]

Cyber espionage is only one component of China's technology-acquisition efforts. The combination of the dual-use nature of most in-demand commercial technologies and China's geopolitical and economic rise means that China can capture innovative new technologies, know-how, and processes through a range of licit and transparent means as well.

A May 2019 report from the US-China Economic and Security Review Commission highlighted six principal means through which China acquires technology from US companies: foreign direct investment/company acquisition, venture capital investments, joint ventures, licensing agreements, talent acquisition, and cyber espionage.[188] Previously, the US Defense Security Services listed the use of irregular collectors at conferences and trade shows as another particularly effective and prominent method,[189] while other analysts and government agencies have cited methods such as open source exploitation, leveraging China's dual-use space program, and direct solicitation.[190]

The totality of China's technology acquisition program constitutes an impressive mixture of legal and illicit, transparent and surreptitious, collaborative and manipulative, further complicating the challenge associated with protecting US AI and enabling technologies.

From a counterintelligence perspective China, again in the words of FBI Director Wray, "represents the broadest, most pervasive, most threatening challenge we face as a country." However, it is not the *only* challenge to technology protection. Other state and non-state actors are working to acquire the innovation outputs of the global leading US high-tech industry and best-in-class US applied research and academic communities. Russia's Zhores supercomputer is an indicative and instructive example: The first to be devoted to "solving problems in the field of artificial intelligence," it is largely built on Western technology. The program actually began at an institute founded in conjunction with the Massachusetts Institute of Technology.[191]

Recommendations to protect US technology clearly overlap with other components of this recommended strategy, most notably compete and engage. Additional recommendations include:

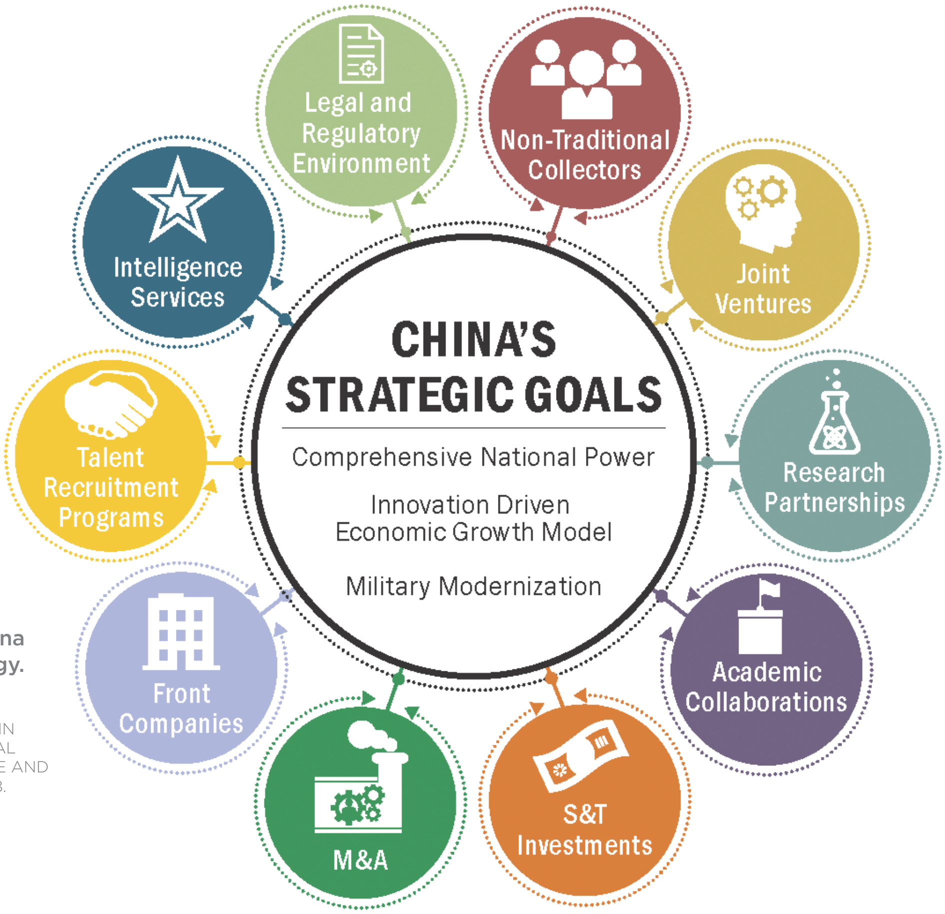


Figure 7: A list of methods through which China acquires technology.

SOURCE: "FOREIGN ECONOMC ESPIONAGE IN CYBERSPACE," NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER, 2018.

ODNI-created material in the public domain, including ODNI's official presences on social media sites, may be copied, distributed, and reproduced without obtaining ODNI permission. When such information is copied, distributed or reproduced, it is appropriate to cite ODNI or the relevant ODNI component or office as the source of the information.

Department of Justice APT-10 Indictment

The indictment stated that from at least 2006–2018, the two individuals of interest "conducted extensive campaigns of global intrusions into computer systems aiming to steal, among other data, intellectual property and confidential business and technological information from more than at least forty five commercial and defense technology companies."

- **Enlisting support by raising awareness and crafting narratives.** The United States is not the only country in the world concerned about China's systematic theft of commercial and military technology and its implications for economic and national security or technology diffusion issues. Significantly, the December 2018 Department of Justice "name-and-shame" indictment of two Chinese hackers suspected of being part of a Chinese group known as Advanced Persistent Threat 10 (APT-10) identified eleven other countries affected by APT-10's technology theft efforts, including many close US allies and the largest trading partners of the United States.[192]

  What should be a priority is crafting narratives and accompanying incentives—rather than overreliance on so-called sticks—that offer opportunities for US allies and partners to evaluate the security implications of doing business with Chinese high-tech companies. Efforts to collaborate with US allies and partners to build capacity in cybersecurity and other methods of technology protection should also be pursued.

  The ongoing efforts to dissuade European allies, in particular, from doing business with Huawei have achieved mixed results, but should be continued and extended to other companies on a case-by-case basis.

  Some targeted states have begun to reconsider their commercial engagement with Huawei, suspected of being an important cog in the wheel of China's surreptitious acquisition of sensitive technologies. Poland, for example, arrested two Huawei executives on suspicions of technology theft and is reportedly set to exclude Huawei from future 5G network plans.[193] Other states continue engagement, though with an enhanced understanding of the risks associated with this engagement.

- **IP protection.** The United States must invest in programs that encourage strong IP protection, not just domestically but also abroad. Strong IP protection does lead to great prosperity over the long term, but many countries in the developing world do not view it that way. Rather, they perceive IP protection as a virtual monopoly that induces high prices and prevents their products from competing with the developed world.

  The US federal government can enable an effective IPR system that not only outlines the rules and the penalties for violations of IPR, but also the effective management and policing of the current system. This is partly a funding issue but also a matter of priority within the Executive Office of the President and Congress. Working with the US Trade Representative, major funders of IP like the DoD and National Institutes of Health, and other major domestic sources of IP, the federal government can more nimbly act on limiting transfers of AI technology, source code, as well as encryption keys to countries that have similar policies that respect the IPR regime.

- **Safeguard "patriotic" investors.** The recent announcement of a Pentagon mission to pursue and vet patriotic investors by Undersecretary Ellen Lord has relevance to AI development.[194] The program, now known as the Trusted Capital Marketplace, is designed to identify innovations in the US technology ecosystem that should be protected, to identify which investors are not vulnerable personally or institutionally to adversarial investment, and to work with both to ensure financial arrangements are made that benefit US national security. While the program is in its infancy, the Department of Defense should invest significantly and work closely with the Department of the Treasury as well as the Securities and Exchange Commission in order to ensure that defense-critical technologies, either government or commercially developed, are protected and promoted from adversarial capital.

LIN ZHIZHAO/UNSPLASH

CONCLUSION

AI is at the center of the future of the 4IR and the promise that the fusion of the physical and digital world portends.

Development, deployment, and diffusion of more robust AI technologies is certain to accelerate—creating tangible benefits for the global economy and for the provision of public-sector services, including those that can enhance US and allied security.

With this promise, though, comes a degree of peril—or, at the least, new and enhanced societal, political, ethical, and security challenges. AI's potent, but uncertain, effects on the global strategic context and geopolitical competition is already expanding the dimensions of threats to the security, stability, and prosperity of the United States and its allies and partners.

For militaries around the world—including US competitors—AI technologies are being harnessed to improve readiness and decision-making and to introduce novel capabilities that can create durable strategic, operational, and tactical asymmetries and advantages. Competition to develop cognitive capabilities will introduce destabilizing dynamics into already escalating geopolitical and military domain area competitions. AI technologies will be used—already are being used—to exploit the vulnerabilities of the digital age and pose difficult to detect and deter threats to the stability and efficacy of US and allied societies and polities. Furthermore, the scaled and systemic use of AI in unethical or authoritarian ways by both non-state and, especially, state actors poses a pervasive threat to the liberal values and norms on which the US legal and political system are based and, as a result, to US and allied individual and collective interests.

Establishing and sustaining US leadership in AI technology and in norms for AI use, safety, and ethics is an urgent national security priority that radiates beyond the interests and responsibilities of DoD or even solely the USG. Fortunately, urgency does not yet equate to desperation. The US still holds advantages, assets, incentives, and relationships that can be deployed—and must be protected—to mitigate risks to and capitalize on opportunities for US security, stability, and prosperity.

Doing so requires a government-led strategy that builds on the varied frameworks already articulated to identify and pursue specific investment priorities, and is bolstered by the recognition that the most acute ethics, safety, and security challenges of a competitive, anxious, and dual-use context—and capabilities to meet them—are shared across government, with industry, and among allies and partners around the world.

ABOUT THE AUTHORS

Mr. Tate Nurkin is the founder of OTH Intelligence Group and a Non-Resident Senior Fellow with the Scowcroft Center for Strategy and Security at the Atlantic Council.

Before establishing OTH Intelligence Group in March 2018, Mr. Nurkin spent twelve years at Jane's by IHS Markit where he served in a variety of roles, including managing Jane's Defense, Risk, and Security Consulting practice. From 2013 until his departure, he served as the founding Executive Director of the Strategic Assessments and Futures Studies (SAFS) Center, which provided thought leadership and customized analysis on global competition in geopolitics, future military capabilities, and the global defence industry. He previously worked for Joint Management Services, the Strategic Assessment Center of SAIC, and the Modeling, Simulation, Wargaming, and Analysis team of Booz Allen Hamilton. From 2014 – 2018 he served consecutive two-year terms on the World Economic Forum's Nuclear Security Global Agenda Council and its Future Council on International Security, which was established to diagnose and assess the security and defense implications of the Fourth Industrial Revolution.

Substantively, Mr. Nurkin's research and analysis has a particularly strong focus on US-China competition, defense technology, the future of military capabilities, and the global defense industry and market issues. He also specializes in the design and delivery of alternative futures analysis exercises such as scenario planning, red teaming, and wargaming.

Tate is a frequent author and speaker on these overlapping research priorities. For example, he was the lead author of the US-China Economic and Security Review Commission's report entitled *China's Advanced Weapons Systems,* which was published in May 2018, and has provided testimony to the Commission on two occasions. In March 2019, he was featured on a Center for Strategic and International Studies *China Power* podcast on China's unmanned systems.

Tate holds a master of science degree in international affairs from the Sam Nunn School of International Affairs at Georgia Tech and a bachelor of arts in history and political science from Duke University. He lives in Charlotte, NC.

Mr. Stephen Rodriguez is the Founding Partner of One Defense, a next generation national security enterprise that leverages machine learning to identify advanced software and hardware commercial capabilities and accelerate their transition into the defense industrial base. He has also served as a Venture Partner supporting the above-market venture portfolio performance of multiple New York and Washington DC venture capital firms.

Mr. Rodriguez began his career at Booz Allen Hamilton shortly before 9/11, supporting their National Security practice. In his capacity as an expert on game theoretic applications, he supported the United States Intelligence Community, Department of Defense, and Department of Homeland Security as a lead architect for the Thor's Hammer, Schriever II/III and Cyber Storm wargames. He subsequently was a Vice President at a artificial intelligence company (Sentia Group) and served as Chief Marketing Officer for an international defense corporation (NCL Holdings).

Mr. Rodriguez serves as a Board Director or Board Advisor of eight venture-backed companies (Duco, HatchApps, HighSide, ODL Services, Omelas, Uniken, Vantage Robotics, and WarOnTheRocks) as well as four non-profit organizations (Daniel Morgan Graduate School, Next Defense, Public Spend Forum, and Training Leaders International). He is also Senior Advisor at the Atlantic Council and the Senior Innovation Advisor at the Naval Postgraduate School.

Mr. Rodriguez received his B.B.A degree from Texas A&M University and an M.A. degree from Georgetown University's School of Foreign Service. He is published in *Foreign Policy, WarOnTheRocks, National Review,* and *RealClearDefense.* Notably, his graduate thesis on conflict resolution in the Caucasus resulted in an invitation to join incoming Secretary of Defense Robert Gates transition team in late 2006. Mr. Rodriguez resides in Washington D.C. with his wife, Laura, a venture capitalist with Bulldog Innovation Group and their children, Fletcher, Violet, and Pierce.

ACKNOWLEDGMENTS

We would like to thank Andrew Gonzalez for his research and fact-checking on early drafts of this report. We would also like to thank Anca Agachi for her tireless support in seeing this Strategy Paper through the production process, as well as the associated launch event. Finally, this would not be possible without the faithful support of the Scowcroft Center leadership comprised of Barry Pavel and Matthew Kroenig.

Any errors or omissions are the sole responsibility of the authors. The Atlantic Council does not take institutional positions.

Endnotes

1 Carl Sagan and Ann Druyan, *The Demon-Haunted World: Science as a Candle in the Dark* (New York: Random House, 1996), 60.

2 Klaus Schwab, "The Fourth Industrial Revolution," a speech given at the World Economic Forum, January 3, 2017.

3 Michio Kaku, "The Future in Light of the 4IR," a speech given at the International Defence Conference, Abu Dhabi, February 14, 2019.

4 "Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan," translated and posted by the Foundation for Law and International Affairs, https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf.

5 Tim Dutton, "An Overview of National AI Strategies," *Medium,* June 28, 2019, https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd.

6 Press release, Office of Senator Martin Heinrich, https://www.heinrich.senate.gov/press-releases/heinrich-portman-schatz-propose-national-strategy-for-artificial-intelligence-call-for-22-billion-investment-in-education-research-and-development.

7 White House executive order of February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/. Exec. Order No. 13,859, 84 C.F.R. 3967 (February 14, 2019, http://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf.

8 "DoD Takes Strategic Approach to Artificial Intelligence," US Department of Defense, February 12, 2019, https://www.defense.gov/explore/story/Article/1755991/dod-takes-strategic-approach-to-artificial-intelligence/.

9 *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity,* Department of Defense, February 2019.

10 "AI Next Campaign," DARPA website, accessed March 2019, https://www.darpa.mil/work-with-us/ai-next-campaign.

11 *The Global Strategic Trends Report: The Future Starts Today,* UK Ministry of Defence, Sixth Edition, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf.

12 *China's Military Strategy,* State Council of the People's Republic of China, http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

13 Mingda Qiu, *China's Science of Military Strategy: Cross-Domain Concepts in the 2013 Edition,* Cross-Domain Deterrence working paper, University of California, San Diego, September 2015, 4, http://deterrence.ucsd.edu/_files/Chinas%20Science%20of%20Military%20Strategy%20Cross-Domain%20Concepts%20in%20the%202013%20Edition%20Qiu2015.pdf.

14 Andrew Monaghan, *The New Russian Foreign Policy Concept: Evolving Continuity,* Chatham House, April 2013, https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0413pp_monaghan.pdf.

15 *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge,* Department of Defense, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

16 Jeremy Chao, "China May Be Experiencing Negative GDP Growth, Says Senior Economist," *Epoch Times,* December 20, 2018, https://www.theepochtimes.com/china-may-be-experiencing-negative-gdp-growth-says-senior-economist_2744261.html.

17 Elsa Kania, "AlphaGo and Beyond: The Chinese Military Looks to Future 'Intelligentized' Warfare," *Lawfare,* June 5, 2017, https://www.lawfareblog.com/alphago-and-beyond-chinese-military-looks-future-intelligentized-warfare.

18 Tom Barnes, "China Tests Army of Tiny Drone Ships That Can 'Shark Swarm' Enemies during Sea Battles," *Independent,* June 7, 2018, https://www.independent.co.uk/news/world/asia/china-drone-ships-unmanned-test-video-military-south-sea-shark-swarm-a8387626.html.

19 Gregory C. Allen, "Understanding China's AI Strategy," Center for a New American Security, February 6, 2019, https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

20 Louis Columbus, "How China is Dominating Artificial Intelligence," *Forbes,* December 16, 2018, https://www.forbes.com/sites/louiscolumbus/2018/12/16/how-china-is-dominating-artificial-intelligence/#29dc67b72b2f.

21 "International Tech Giants to Establish AI Centers in Shanghai," *China Daily* via Xinhua, September 18, 2018, http://global.chinadaily.com.cn/a/201809/18/WS5b9fed39a31033b4f4656891.html.

22 Tara Francis Chan, "FBI Director Says China Is the 'Broadest, Most Significant' Threat to the US and Says Its Espionage Is Active in All 50 States," *Business Insider,* July 19, 2018, https://www.businessinsider.com/fbi-director-says-china-is-the-broadest-most-significant-threat-to-the-us-2018-7.

23 The authors acknowledge that quantum computing is at a relatively early stage of development and that the US government has made considerable commitments in funding to quantum science since 2017. This assessment reflects developments to date.

24 The term "little green men" is frequently used to describe Russian soldiers who were deployed to Crimea with unmarked green uniforms during the Russian campaign to assert

sovereignty over the territory of Ukraine.

25 Samuel Bendett, “Autonomous Robotic Systems in the Russian Armed Forces,” *Mad Scientist Laboratory* blog, February 11, 2019, https://madsciblog.tradoc.army.mil/tag/uran-9/.

26 Samuel Bendett, “In AI, Russia Is Hustling to Catch Up,” *Defense One,* April 4, 2018, https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/.

27 Valeria Shmyrova, “The Market for Artificial Intelligence in Russia Is Estimated at $700 million,” *CNews,* November 27, 2019, http://www.cnews.ru/news/top/2017-11-27_rynok_iskusstvennogo_intellekta_v_rossii_otsenivaetsya.

28 Bendett, “In AI, Russia Is Hustling.”

29 Analysis is derived from Samuel Bendett, “Here’s How the Russian Military Is Organizing to Develop AI,” *Defense One,* July 20, 2018, https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/.

30 Margarita Konav, “Thoughts on Russia’s AI Strategy,” Center for Security and Technology, Georgetown University Walsh School of Foreign Service, October 30, 2019, https://cset.georgetown.edu/2019/10/30/russias-ai-strategy/.

31 Robert Kagan, “The Strongmen Strike Back,” *Washington Post,* March 14, 2019, https://www.washingtonpost.com/news/opinions/wp/2019/03/14/feature/the-strongmen-strike-back/?utm_term=.7c63e2743bb4.

32 Kagan, “The Strongmen Strike Back.”

33 Richard Fontaine and Kara Frederick, “The Autocrat’s Tool Kit,” *Wall Street Journal,* March 15, 2019, https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637.

34 Fontaine and Frederick, “The Autocrat’s Tool Kit.”

35 Samuel Bendett, “Moscow to Weave AI Face Recognition into Its Urban Surveillance Net,” *Defense One,* May 14, 2019, https://www.defenseone.com/technology/2019/05/moscow-weave-ai-face-recognition-its-urban-surveillance-net/156994/.

36 Jakob Reimann, “China Is Flooding the Middle East With Cheap Drones,” *Foreign Policy in Focus,* February 18, 2019, https://fpif.org/china-is-flooding-the-middle-east-with-cheap-drones/.

37 Andrew Kramer, “Russian General Pitches Information Operation as a Form of War,” *New York Times,* March 2, 2019, https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html.

38 Dave Johnson, “General Gerasimov on the Vectors of the Development of Military Strategy,” a review of the general’s speech of March 2, 2019, at the Russian Academy of Military Science, NATO Defense College website, last updated March 30, 2019, http://www.ndc.nato.int/research/research.php?icode=585.

39 Inskit Group, “Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion,” Recorded Future, March 6, 2019, https://www.recordedfuture.com/china-social-media-operations/.

40 Thirty million connected items is an aggregate of predictions from IHS Markit, Ericsson, and IDC. Source: Amy Nordrum, “Popular Internet of Things Prediction of 50 Billion Devices by 2020 Is Outdated,” *IEEE Spectrum,* August 18, 2016, https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.

41 Fontaine and Frederick, “The Autocrat’s Tool Kit.”

42 “On Truth and Lies in the Nonmoral Sense,” *The Portable Nietzsche,* ed. Walter Kaufmann (New York: Viking Press, 1954), 45.

43 Lyrics from “The Boxer,” written by Paul Simon, performed by Simon and Art Garfunkel, released in 1969, https://www.youtube.com/watch?v=wzUEL7vw60U.

44 *Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for US National Security,* a minority staff report prepared for the use of the US Senate Committee on Foreign Relations, January 10, 2018, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

45 Tate Nurkin et al., *China’s Advanced Weapons Systems,* Jane’s by IHS Markit, published by the US-China Economic and Security Review Commission, May 2018, https://www.uscc.gov/sites/default/files/Research/Jane%27s%20by%20IHS%20Markit_China%27s%20Advanced%20Weapons%20Systems.pdf.

46 This list is focused exclusively on AI-enabled military/operational capabilities and does not include business process optimization, which was a specific area of focus identified in the DoD AI Strategy paper.

47 Terri Moon Cronk, “DoD Unveils Its Artificial Intelligence Strategy,” US Department of Defense, February 12, 2019, https://dod.defense.gov/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/.

48 Marcus Weisgurber, “Project Maven: The Pentagon’s New Artificial Intelligence Has Been Hunting Terrorists for Months,” *Defense One* video, posted on YouTube on March 30, 2018, https://www.youtube.com/watch?v=5UfF121mFiQ.

49 Jon Harper, “Air Force Leader: Artificial Intelligence Could Help Monitor Social Media,” *National Defense Magazine,* July 26, 2017, http://www.nationaldefensemagazine.org/articles/2017/7/26/air-force-leader-artificial-intelligence-could-help-monitor-social-media.

50 Harper, “Air Force Leader: Artificial Intelligence Could Help Monitor Social Media.”

51 Cortney Weinbaum and John N.T. Shanahan, “Intelligence in a Data-Driven Age,” *Joint Forces Quarterly,* Vol. 90, Third Quarter 2018, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-90/jfq-90.pdf.

52 Jonathan Vanian, “Defense Department Is Using Google’s AI Tech to Help Drone Surveillance,” *Fortune,* March 6, 2019, http://fortune.com/2018/03/06/google-department-defense-drone-ai/.

53 Lee Fang, “Google Hedges on Promise to End Controversial Involvement in Military Drone Contract,” *Intercept,* March 1, 2019, https://theintercept.com/2019/03/01/google-project-maven-contract/.

54 Marcus Weisgerber, “General: Project Maven Is Just the Beginning of Military’s Use of AI,” *Defense One,* June 28, 2018, https://www.defenseone.com/technology/2018/06/general-project-maven-just-beginning-militarys-use-ai/149363/.

55 Master Sergeant Joshua Strang, “AETC Explores Learning Possibilities through New Pilot Training,” Air Education and Training Center, De-

cember 7, 2017, https://www.aetc.af.mil/News/Article/1391431/aetc-explores-learning-possibilities-through-new-pilot-training-program/.

56 Strang, "AETC Explores Learning Possibilities."

57 Yasmin Tadjdeh, "Big Data, AI to Advance Modeling and Simulation," *National Defense,* January 3, 2018, http://www.nationaldefensemagazine.org/articles/2018/1/3/big-data-ai-to-advance-modeling-and-simulation.

58 "EDA Studies Points [sic] Towards Big Data Potential for Defense," European Defence Agency, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/12/18/eda-studies-points-towards-big-data-potential-for-defence.

59 "EDA Studies," European Defence Agency.

60 Elsa B. Kania, *Learning Without Fighting: New Developments in PLA Artificial Intelligence War-Gaming,* Jamestown Foundation, China Brief, Vol. 19, No. 7, https://jamestown.org/program/learning-without-fighting-new-developments-in-pla-artificial-intelligence-war-gaming/.

61 Kania, *Learning Without Fighting*.

62 Stephen Chen, "China Military Develops Robotic Submarines to Launch a New Era of Sea Power," *South China Morning Post,* July 22, 2018, https://www.scmp.com/news/china/society/article/2156361/china-developing-unmanned-ai-submarines-launch-new-era-sea-power.

63 David B. Larter, "A Classified Pentagon Maritime Drone Program Is About to Get Its Moment in the Sun," *Defense News,* March 14, 2019, https://www.defensenews.com/naval/2019/03/14/a-classified-pentagon-maritime-drone-program-is-about-to-get-its-moment-in-the-sun/.

64 "Autonomous Weapons: an Open Letter from AI & Robotics Researchers," Future of Life Institute, July 28, 2015, https://futureoflife.org/open-letter-autonomous-weapons/.

65 Justin Rohrlich, "The US Army Wants to Turn Tanks into AI-powered Killing Machines," *Quartz,* February 26, 2019, https://qz.com/1558841/us-army-developing-ai-powered-autonomous-weapons/.

66 Kelley M. Sayler, *Artificial Intelligence and National Security,* Congressional Research Service, January 30, 2019, 18.

67 Rohrlich, "The US Army Wants to Turn Tanks."

68 Patrick Tucker, "US Military Changing 'Killing Machine' Robo-tank Program After Controversy," *Defense One,* March 1, 2019, https://www.defenseone.com/technology/2019/03/us-military-changing-killing-machine-robo-tank-program-after-controversy/155256/.

69 Erik Slavin, "Pentagon Unveils Perdix Micro-drone Swarm," *Stars and Stripes,* January 10, 2017, https://www.stripes.com/news/pentagon-unveils-perdix-micro-drone-swarm-1.448124.

70 Erik Slavin, "Pentagon Unveils Perdix Micro-drone Swarm," *Stars and Stripes,* January 10, 2017, https://www.stripes.com/news/pentagon-unveils-perdix-micro-drone-swarm-1.448124.

71 "Gavin Williamson's Brain Has Gone Absent Without Leave," opinion piece, *Guardian,* February 11, 2019, https://www.theguardian.com/commentisfree/2019/feb/11/gavin-williamson-defence-policy-uk.

72 Chloe Taylor, The British Army Is to Invest $44 Million in a Fleet of Tiny Hand-sized Drones," CNBC, March 6, 2019, https://www.cnbc.com/2019/03/06/the-british-army-is-to-invest-44-million-in-a-fleet-of-tiny-drones.html.

73 Nikolai Novichkov, "Air Show China 2018: Norinco Presents UAV Swarm Concept," *Jane's Defence Weekly,* November 9, 2018, https://www.janes.com/article/84438/airshow-china-2018-norinco-presents-uav-swarm-concept.

74 Andrew Tate, "China Launches Record-breaking UAV Swarm," *Jane's Defence Weekly,* 21 June 2017, https://janes.ihs.com/Janes/Display/jdw66273-jdw-2017.

75 James Drew, "Pentagon Touts 'Loyal Wingman' for Combat Jets," *Flight Global,* March 30, 2016, https://www.flightglobal.com/news/articles/pentagon-touts-loyal-wingman-for-combat-jets-423682/.

76 The term is commonly used to describe unmanned systems that are developed and procured at a low enough cost and in sufficient numbers that they can be deployed to contested environments and potentially lost in these environments without risk of a strategically significant impact on limited budgets or operational effectiveness.

77 Valerie Insinna, "Introducing Skyborg, Your New AI Wingman," March 14, 2019, *C4ISRNet,* https://www.c4isrnet.com/air/2019/03/14/introducing-skyborg-your-new-ai-wingman/. David Axe, "Meet the XQ-58A Valkyrie: The Air Force's New Stealth Wonder Weapon," *National Interest,* March 7, 2019, https://nationalinterest.org/blog/buzz/meet-xq-58a-valkyrie-air-forces-new-stealth-wonder-weapon-46407.

78 Amrita Khalid, "The Air Force Is Exploring AI-Powered Autonomous Drones," March 27, 2019, *Engadget,* https://www.engadget.com/2019/03/27/the-air-force-is-exploring-ai-powered-autonomous-drones/.

79 Jillian Eugenios, "Ray Kurzweil: Humans Will Be Hybrids by 2030," CNN.com, June 4, 2015, https://money.cnn.com/2015/06/03/technology/ray-kurzweil-predictions/index.html.

80 DARPA OFFset Program Calls for Third Swarm Sprint, DARPA video posted October 12, 2018, on YouTube, https://www.youtube.com/watch?v=2S3gmLZoYBQ.

81 DARPA OFFset Program Calls for Third Swarm Sprint, DARPA.

82 "DIA's Ashley Details Challenges and Shifts in Defense Intelligence," *Defense and Aerospace Report,* October 2018, https://defaeroreport.com/2018/10/09/dias-ashley-details-challenges-and-shifts-in-defense-intelligence/.

83 Patrick, Tucker, "Defense Intel Chief Worried About Chinese 'Integration of Human and Machines'", *Defense One,* October 10, 2018, https://www.defenseone.com/technology/2018/10/defense-intel-chief-worried-about-chinese-integration-human-and-machines/151904/

84 "Certification Testing of First Combat Exoskeleton to Be Over by 2020," Tass, 21 January 2019, http://tass.com/science/1040988.

85 "US Army NSRDEC Awards Contract to Lockheed for ONYX Exoskeleton," Army Technology, November 30, 2018, https://www.army-technology.com/news/nsrdec-lockheed-onyx-exoskeleton/.

86 Patrick Tucker, "Russia, US are in a Military Exoskel-

eton Race," *Defense One,* August 30, 2018, https://www.defenseone.com/technology/2018/08/russia-us-are-military-exoskeleton-race/150939/.

87 Bryan Christiansen, "The Use of AI and VR in Maintenance Management," Engineering.com, accessed February 22, 2019, https://www.engineering.com/AdvancedManufacturing/ArticleID/18100/The-Use-of-AI-and-VR-In-Maintenance-Management.aspx.

88 Cronk, "DOD Unveils Its Artificial Intelligence Strategy."

89 J.R. Wilson, "Today's Battle for the Electromagnetic Spectrum," *Military and Aerospace Electronics* (2016) 27: 8, http://www.militaryaerospace.com/articles/print/volume-27/issue-8/special-report/today-s-battle-for-the-electromagnetic-spectrum.html.

90 Monica Alleven, "NIST Taps AI for Better Radar Detection in 3.5 GHz Bandwidth," *FierceWireless,* February 21, 2019, https://www.fiercewireless.com/wireless/nist-taps-ai-for-better-radar-detection-3-5-ghz-band.

91 Alleven, "NIST Taps AI."

92 Ryan Browne, "Russia Jammed GPS during Major NATO Military Exercise with US Troops," CNN, November 14, 2018, https://www.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html.

93 Valeria Insinna, "Pentagon Looks to Adaptive EW Solutions to Thwart Future Adversaries," *Defense News,* August 28, 2016, https://www.defensenews.com/air/2016/08/29/pentagon-looks-to-adaptive-ew-systems-to-thwart-future-adversaries/.

94 "Electronic Warfare Development Targets Fully Adaptive Threat Response Technology," Georgia Institute of Technology, August 15, 2013, http://www.rh.gatech.edu/news/228881/electronic-warfare-development-targets-fully-adaptive-threat-response-technology.

95 Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation,* a report of the University of Oxford's Future of Humanity Institute, University of Cambridge's Centre for the Study of Existential Risk, Center for a New American Security, Electronic Frontier Foundation, and OpenAI, February 2018, https://arxiv.org/pdf/1802.07228.pdf.

96 Brundage et al., *The Malicious Use of Artificial Intelligence.*

97 Philung Kirat, Jiyong Jang, and Marc Ph. Stoecklin, "DeepLocker: Concealing Targeted Attacks with AI Locksmithing," IBM Research, BlackHat 2018 Presentation, https://i.blackhat.com/us-18/Thu-August-9/us-18-Kirat-DeepLocker-Concealing-Targeted-Attacks-with-AI-Locksmithing.pdf.

98 Joseph Menn, "New Genre of Artificial Intelligence Programs Take Computer Hacking to Another Level," Reuters, August 8, 2018, https://ca.reuters.com/article/technologyNews/idCAKBN1KT120-OCATC.

99 Nicolas Fearn, "How AI Will Underpin Cyber Security in the Next Few Years," *ComputerWeekly.com,* February 2018, https://www.computerweekly.com/feature/How-AI-will-underpin-cyber-security-in-the-next-few-years.

100 Francois Chollet, "What Worries Me About AI," *Medium,* March 28, 2018, https://medium.com/@francois.chollet/what-worries-me-about-ai-ed9df072b704.

101 Weinbaum and Shanahan, "Intelligence in a Data-Driven Age."

102 "Fake Obama Created Using AI Video Tool," BBC News, streamed on YouTube, https://www.youtube.com/watch?v=AmUC4m6w1wo.

103 Cecilia Kang, "Nancy Pelosi Criticizes Facebook Handling of Altered Videos," *New York Times,* May 29, 2019, https://www.nytimes.com/2019/05/29/technology/facebook-pelosi-video.html.

104 Jill Aitoro, "Forget Project Maven. Here Are a Couple of Other DoD Projects Google Is Working On," *C4ISRNet,* March 13, 2019, https://www.c4isrnet.com/it-networks/2019/03/13/forget-project-maven-here-are-a-couple-other-dod-projects-google-is-working-on/.

105 Catherine Stupp, "Fraudster Used AI to Mimic CEO's Voice in Unusual Cybercrime Case," *Wall Street Journal,* August 30, 2019, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

106 Drew Harrell, "An Artificial Intelligence First: Voice-mimicking Software Reportedly Used in Major Theft," *Washington Post,* September 4, 2109, https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/.

107 Stupp, "Fraudster Used AI."

108 "Attacking Machine Learning with Adversarial Examples," *OpenAI,* February 24, 2017, https://openai.com/blog/adversarial-example-research/.

109 Patrick Tucker, "The Newest AI-Enabled Weapons: 'Deep-Faking' Photos of Earth," *Defense One,* March 31, 2019, https://www.defenseone.com/technology/2019/03/next-phase-ai-deep-faking-whole-world-and-china-ahead/155944/.

110 "John F. Kennedy Moon Speech-Rice Stadium, September 12, 1962," text and video clip, Johnson Space Center, NASA, https://er.jsc.nasa.gov/seh/ricetalk.htm.

111 Gabrielle Caron, "How Taylor Swift Showed Us the Scary Future of Facial Recognigtion," *Guardian,* February 15, 2019, https://www.theguardian.com/technology/2019/feb/15/how-taylor-swift-showed-us-the-scary-future-of-facial-recognition.

112 Niraj Choksi, "Facial Recognition's Many Controversies, from Stadium Security to Racist Software," *New York Times,* May 15, 2019, https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html.

113 "Smart Lie-detection System to Tighten EU's Busy Borders," European Commission website, October 24, 2018, http://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726.

114 Patrick Tucker, "European Countries to Test AI Border Guards," *Defense One,* November 1, 2018, http://www.defenseone.com/technology/2018/11/european-countries-test-ai-border-guards/152511/.

115 "Smart Lie-detection System," European Commission website.

116 Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame, and Lots of Cameras," *New York Times,* July 18, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[117] Paul Mozur, “One Month, 500,000 Facial Scans: How China Is Using A.I. to Profile a Minority,” *New York Times,* April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[118] Mozur, “One Month, 500,000 Facial Scans.”

[119] Mozur, “Inside China’s Dystopian Dreams.”

[120] “Chinese Facial Recognition Database Inadvertently Exposed,” Soufan Group, March 1, 2019, https://thesoufancenter.org/?s=China+facial+recognition.

[121] Je Shan, “China Exports Facial ID Technology to Zimbabwe,” *Global Times,* April 12, 2018, http://www.globaltimes.cn/content/1097747.shtml.

[122] Jory Heckman, “Trump Signs Executive Order Fostering Artificial Intelligence R&D in Government,” *Federal News Network,* February 11, 2019, https://federalnewsnetwork.com/artificial-intelligence/2019/02/trump-signs-executive-order-fostering-ai-rd-in-government/.

[123] Exec. Order No. 13,859, 84 C.F.R. 3967 (February 14, 2019), http://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf.

[124] Jory Heckman, “White House Science Chief: ‘We Don’t Really Have a Clue’ About Number of AI Researchers,” *Federal News Network,* February 19, 2019, https://federalnewsnetwork.com/artificial-intelligence/2019/02/white-house-science-chief-we-dont-really-have-a-clue-about-number-of-ai-researchers/.

[125] Shaun Wateman, “DOD’s New AI Center Ramps Up,” *Air Force Magazine,* May 17, 2019, http://www.airforcemag.com/Features/Pages/2019/May%20 2019/DODs-New-AI-Center-Ramps-Up.aspx.

[126] Jamie McIntyre and Travis Tritton, “Sweeping Pentagon Review Shows America’s Defense Industrial Base in Decline,” *Washington Examiner,* October 5, 2018, https://www.washingtonexaminer.com/sweeping-pentagon-review-shows-americas-defense-industrial-base-in-decline.

[127] Marty Skovlund Jr., “The Military’s 5 Biggest Procurement Fails Since 9/11,” *Task and Purpose,* March 31, 2017, https://taskandpurpose.com/military-procurement-fails-9-11/.

[128] Molly Oswaks, “US Army’s Pixellated Camo Uniform Is a $5 Billion Failure,” *Gizmodo,* June 26, 2012, https://gizmodo.com/5921291/us-armys-pixellated-camo-uniform-is-a-5bil-failure.

[129] Skovlund, “The Military’s 5 Biggest Procurement Fails.”

[130] Christopher G. Pernin et al., *Lessons from the Army’s Future Combat Systems Program,* RAND Corporation, 2012, https://www.rand.org/pubs/monographs/MG1206.html.

[131] Joel Wuthnow and Phillip Saunders, “China’s Military Has a Discipline Problem: Here Is How Xi Jinping Is Trying to Fix It, *National Interest,* April 12, 2017, https://nationalinterest.org/feature/chinas-military-has-discipline-problem-here-how-xi-jinping-23163.

[132] Joseph Trevithick and Tyler Rogoway, “No, Russia’s Su-57 Stealth Fighter Program Isn’t Dead, at Least Not Yet,” *Drive,* July 18, 2018, http://www.thedrive.com/the-war-zone/22234/no-russias-su-57-stealth-fighter-program-isnt-dead-at-least-not-yet.

[133] “In China, Consumers Are Becoming More Anxious About Data Privacy,” *Economist,* January 25, 2018, https://www.economist.com/china/2018/01/25/in-china-consumers-are-becoming-more-anxious-about-data-privacy.

[134] “Why China’s AI Push is Worrying,” *Economist,* July 27, 2017, https://www.economist.com/news/leaders/21725561-state-controlled-corporations-are-developing-powerful-artificial-intelligence-why-chinas-ai-push.

[135] Andy Boxall, “WeChat Reaches 963 Million Monthly Active Users; Prepares to Reach a Billion in 2017,” *Business of Apps,* August 23, 2017, http://www.businessofapps.com/wechat-reaches-963-million-monthly-active-users-prepares-to-pass-a-billion-in-2017/.

[136] David Reinsel, John Gantz, and John Rydring, *Data Age 2025: The Digitization of the World: From Edge to Core,* IDC, November 2018, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

[137] IDC defines global datasphere as including traditional and cloud data centers, enterprise-hardened infrastructure such as cell towers, and endpoints including personal computers, smart phones, and Internet of Things devices. Reinsel, Gantz, and Rydring, *Data Age 2025.*

[138] Exec. Order No. 13,859, 84 C.F.R. 3967 (February 14, 2019), http://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf.

[139] Amy Zegart, “The Divide Between Silicon Valley and Washington Is a National-Security Threat,” commentary by the codirector of Stanford University’s Center for International Security and Cooperation, *Defense One,* December 16, 2018, https://www.defenseone.com/ideas/2018/12/divide-between-silicon-valley-and-washington-national-security-threat/153562/?oref=DefenseOneTCO.

[140] Zachary Fryer-Biggs, “Inside the Pentagon’s Plan to Win Over Silicon Valley’s AI Experts,” produced in partnership with the Center for Public Integrity and published in *Wired,* December 21, 2018, https://www.wired.com/story/inside-the-pentagons-plan-to-win-over-silicon-valleys-ai-experts/.

[141] Kevin Roose, “Why Napalm Is a Cautionary Tale for Tech Giants Pursuing Military Contracts,” *New York Times,* March 4, 2019, https://www.nytimes.com/2019/03/04/technology/technology-military-contracts.html.

[142] Fryer-Biggs, “Inside the Pentagon’s Plan to Win Over Silicon Valley’s AI Experts.”

[143] Paul McLeary, “Pentagon Frustrated by Silicon Valley Rejection: Joint Chiefs Chairman,” *Breaking Defense,* November 17, 2018, https://breakingdefense.com/2018/11/pentagon-frustrated-by-googles-rejection/.

[144] Charles Riley and Samuel Burke, “Microsoft CEO Defends US Military Contract That Some Employees Say Crosses a Line,” CNN Business, February 25, 2019, https://www.cnn.com/2019/02/25/tech/augmented-reality-microsoft-us-military/index.html.

[145] Drew Harwell, “San Francisco Becomes First City in U.S. to Ban Facial-recognition Software,” *Washington Post,* May 14, 2019, https://www.washingtonpost.com/technology/2019/05/14/san-francisco-becomes-first-city-us-ban-facial-recognition-software/?utm_term=.2bf101069e44.

[146] Patrick Tucker, “US Military Changing ‘Killing Machine’ Robo-tank Program after Controversy,” *Defense One,* March 1, 2019, https://

www.defenseone.com/technology/2019/03/us-military-changing-killing-machine-robo-tank-program-after-controversy/155256/.

147 Ali Winston, “Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policy Technology,” *Verge,* February 27, 2018, https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd.

148 “International Tech Giants to Establish AI Centers in Shanghai,” *China Daily* via Xinhua, September 18, 2018, http://global.chinadaily.com.cn/a/201809/18/WS5b9fed39a31033b4f4656891.html.

149 Jon Grevatt, “China Inaugurates Commission to Lead Civil-Military Integration,” *Jane's Defense Weekly,* June 21, 2017, https://janes.ihs.com/Janes/Display/FG_521331-JDW.

150 Nurkin et al., “China's Advanced Weapons Systems.”

151 Idress Ali and Patricia Zengerle, “Google's Work in China Benefitting China's Military: General,” Reuters, March 14, 2019, https://www.reuters.com/article/us-usa-china-google-idUSKCN1QV296.

152 Maria Krol Sinclair, “Beyond the Whiplash of the ZTE Deal,” Center for Strategic & International Studies, June 8, 2018, http://www.csis.org/analysis/beyond-whiplash-zte-deal.

153 Nurkin et al., “China's Advanced Weapons Systems.”

154 “Developing Data Sharing Agreements,” William T. Gant Foundation, http://rpp.wtgrantfoundation.org/developing-data-sharing-agreements/answers.

155 Lorand Laskai, “Civil-Military Fusion: The Missing Link Behind China's Technological-Military Rise,” Council on Foreign Relations, January 29, 2018, https://www.cfr.org/blog/civil-military-fusion-missing-link-between-chinas-technological-and-military-rise.

156 Nick Bostrom, “Ethical Issues in Advanced Artificial Intelligence,” nickbostrom.com, 2003, https://nickbostrom.com/ethics/ai.html.

157 Sam Shead, “Eric Schmidt: ‘Were the Killer Robots to Start, We Would Find a Way to Stop Them,’ ” *Forbes,* December 11, 2018, https://www.forbes.com/sites/samshead/2018/12/11/eric-schmidt-were-the-killer-robots-to-start-we-would-find-a-way-to-stop-them/#8cfebc9680b0.

158 Sam Shead, “Google Has Developed a ‘Big Red Button’ That Can Be Used to Interrupt Artificial Intelligence to Stop It from Causing Harm,” *Business Insider,* June 3, 2016, https://www.businessinsider.com/google-deepmind-develops-a-big-red-button-to-stop-dangerous-ais-causing-harm-2016-6.

159 Khari Johnson, “China Could Lead World in AI Research in Coming Years, Elsevier Research Finds,” *Venture Beat,* December 11, 2018, https://venturebeat.com/2018/12/11/china-could-lead-world-in-ai-research-in-coming-years-elsevier-report-finds/.

160 “Artificial Intelligence: Commission Takes Forward Its Work on Ethics Guidelines,” European Commission, April 8, 2019, http://europa.eu/rapid/press-release_IP-19-1893_en.htm.

161 "New Ethics Guidelines for Artificial Intelligence Put Citizens at Its Core,” Progressive Standard around ICT for Active and Healthy Ageing,” accessed 2019, https://progressivestandards.org/new-ethics-guidelines-for-artificial-intelligence-put-citizens-at-its-core/.

162 “Mandate for the International Panel on AI,” Prime Minister of Canada Justin Trudeau, December 6, 2018, https://pm.gc.ca/eng/news/2018/12/06/mandate-international-panel-artificial-intelligence.

163 Phoebe Zhang, “China's Top AI Scientist to Drive Development of Ethics Guidelines,” *South China Morning Post,* January 10, 2019, https://www.scmp.com/news/china/science/article/2181573/chinas-top-ai-scientist-drives-development-ethical-guidelines.

164 Zhang, “China's Top AI Scientist.”

165 Outer Space Treaty of 1967, NASA, https://www.state.gov/t/isn/5181.htm.

166 James Vincent, “Putin Says the Nation That Leads AI ‘Will Be the Ruler of the World,’ ”*Verge,* September 4, 2017, https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world.

167 Kai-Fu Lee, “Why China Can Do AI More Quickly and Effectively Than the US,” *Wired,* October 23, 2018, https://www.wired.com/story/why-china-can-do-ai-more-quickly-and-effectively-than-the-us/.

168 Frederick Kempe, “Davos Special Edition: China Seizing AI Lead?,” Atlantic Council, January 26, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/davos-special-edition-china-seizing-ai-lead.

169 “National Defense Technology and Industrial Base Defense Reinvestment and Defense Conversion, http://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part4/chapter148&edition=prelim.

170 Nigel Pittaway, “Boeing Unveils Loyal Wingman Concept Drone,” *Defense News,* February 27, 2019, https://www.defensenews.com/digital-show-dailies/avalon/2019/02/27/boeing-unveils-loyal-wingman-drone/.

171 Paul Jasper Dittrich, “Better Together? Franco-German Cooperation on AI,” Jacques Delors Institute Berlin policy brief, Hertie School of Governance, December 18, 2018, https://www.delorsinstitut.de/2015/wp-content/uploads/2018/12/20181218_Dt-frz-KI_Dittrich_neu.pdf.

172 Robert A. Manning and Peter Engelke with Samuel Klein (contributing author), *Global Innovation Sweepstakes: A Quest to Win the Future,* Atlantic Council, June 2018, https://www.atlanticcouncil.org/wp-content/uploads/2018/06/The-Global-Innovation-Sweepstakes.pdf.

173 *Virtual Battlespace 3* data sheet, Bohemian Interactive Simulations, https://bisimulations.com/products/virtual-battlespace.

174 OpenAI Five, https://openai.com/five/.

175 Michael Zenko, “Millenium Challenge: The Real Story of a Corrupted Military Exercise and Its Legacy,” *War on the Rocks,* November 5, 2015, https://warontherocks.com/2015/11/millennium-challenge-the-real-story-of-a-corrupted-military-exercise-and-its-legacy/.

176 Celia Chen, “China's AI Dreams Stymied by Shortage of Talent, with the US Home to Lion's Share of Experts,” *South China Morning Post,* December 1, 2017, http://www.scmp.com/tech/innovation/article/2122488/chinas-ai-dreams-stymied-shortage-talent-us-home-lions-share-experts. A Chinese-language version of the white paper can be accessed at http://www.tisi.org/Public/Uploads/file/20171201/20171201151555_24517.pdf.

177 Li Qiaoyi, “China Must Overcome Talent Gap to Fulfill AI Ambitions,” January 23, 2018, http://

www.globaltimes.cn/content/1083176.shtml.

178 Tim Dutton, "An Overview of National AI Strategies," *Medium,* June 28, 2018, https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd.

179 Sean O'Connor, "How Chinese Companies Facilitate Technology Transfer from the United States," US-China Economic and Security Review Commission, May 6, 2019, https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf.

180 Yujia He, "How China Is Preparing for an AI-Powered Future," Wilson Briefs, Wilson Center, June 2017, https://www.wilsoncenter.org/publication/how-china-preparing-for-ai-powered-future.

181 Stephen Chen, "China's Brightest Children Are Being Recruited to Develop AI 'Killer Bots,' " *South China Morning Post,* November 8, 2018, https://www.scmp.com/news/china/science/article/2172141/chinas-brightest-children-are-being-recruited-develop-ai-killer.

182 Exec. Order No. 13,859, 84 C.F.R. 3967 (February 14, 2019), http://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf.

183 Cade Metz, "Tech Giants Are Paying Huge Salaries for Scarce A.I. Talent," *New York Times,* October 22, 2017, https://www.nytimes.com/2017/10/22/technology/artificial-intelligence-experts-salaries.html.

184 Cronk, "DoD Unveils Its Artificial Intelligence Strategy."

185 Martin Matishak, "Defense Digital Services Chief Stepping Down After 'Nerd Tour of Duty,' "*Politico,* April 23, 2019, https://www.politico.com/story/2019/04/23/chris-lynch-leaving-defense-digital-1373893.

186 Owen Churchill and Nectar Gan, "China 'Determined to Steal Up Economic Ladder at US' Expense,' FBI Chief Christopher Wray Says," *South China Morning Post,* April 2018, https://www.scmp.com/news/china/politics/article/3007903/china-determined-steal-economic-ladder-us-expense-fbi-chief.

187 Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *Washington Post,* June 8, 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb-28bc52b1_story.html?utm_term=.0432afdddca9.

188 Sean O'Connor, "How Chinese Companies Facilitate Technology Transfer from the United States," US-China Economic and Security Review Commission, May 6, 2019,https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf.

189 "Targeting US Technologies 2017: A Trend Analysis of Cleared Industry Reporting," Defense Security Services, September 7, 2017, https://www.dss.mil/Portals/69/documents/ci/2017_CI_Trends_Report.pdf.

190 Nurkin et al., "China's Advanced Weapons Systems."

191 Samuel Bendett, "Russia's New 'AI Supercomputer' Runs on Western Technology," *Defense One,* March 4, 2019, https://www.defenseone.com/technology/2019/03/russias-new-ai-supercomputer-runs-western-technology/155292/.

192 Indictment: APT-10, Conspiracy to Commit Computer Intrusions, Conspiracy to Commit Wire Fraud, Aggravated Identity Theft, FBI, https://www.fbi.gov/wanted/cyber/apt-10-group.

193 Raymond Zhong, "Huawei Fires Employee Arrested in Poland on Spying Charges," *New York Times,* January 12, 2019, https://www.nytimes.com/2019/01/12/world/asia/huawei-wang-weijing-poland.html.

194 Aaron Metha, "To Counter China, Pentagon Wants to Create Patriotic Investors," March 10, 2019, *Defense News,* https://www.defensenews.com/pentagon/2019/05/10/to-counter-china-pentagon-wants-to-create-patriotic-investors/.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 778-4952
www.AtlanticCouncil.org