

# FUTURE OF DEFENSE TASK FORCE REPORT 2020





**FUTURE OF DEFENSE TASK FORCE**

September 23, 2020

The Honorable Adam Smith  
Chairman  
House Armed Services Committee  
2216 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable William "Mac" Thornberry  
Ranking Member  
House Armed Services Committee  
2216 Rayburn House Office Building  
Washington, D.C. 20515

Dear Chairman Smith and Ranking Member Thornberry:

Thank you for your support in standing up the Future of Defense Task Force. We are pleased to present you with our final report.

Sincerely,



Seth Moulton  
Chair  
Future of Defense Task Force



Jim Banks  
Chair  
Future of Defense Task Force



Susan Davis  
Member of Congress



Scott DesJarlais  
Member of Congress



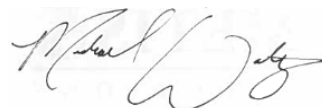
Chrissy Houlahan  
Member of Congress



Paul Mitchell  
Member of Congress



Elissa Slotkin  
Member of Congress



Michael Waltz  
Member of Congress



**TABLE OF CONTENTS**

<b>PROLOGUE .....</b>	<b>1</b>
<b>TASK FORCE MEMBERS .....</b>	<b>3</b>
<b>FINDINGS.....</b>	<b>5</b>
<b>RECOMMENDATIONS .....</b>	<b>7</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>13</b>
<b>EVIDENCE .....</b>	<b>21</b>
<b>EMERGING THREAT STREAMS .....</b>	<b>21</b>
<b>EMERGING TECHNOLOGIES .....</b>	<b>31</b>
<b>PARTNERS AND SECURITY ALLIANCES .....</b>	<b>39</b>
<b>SUPERCHARGING THE INNOVATION BASE.....</b>	<b>45</b>
<b>DEVELOPING A 21<sup>ST</sup> CENTURY WORKFORCE .....</b>	<b>55</b>
<b>FINANCIAL TRADE-OFFS AND ACQUISITION REFORM .....</b>	<b>63</b>
<b>OPERATIONAL CONCEPTS .....</b>	<b>71</b>
<b>BRIEFERS .....</b>	<b>77</b>
<b>HEARINGS &amp; CONGRESSIONAL DELEGATIONS .....</b>	<b>79</b>
<b>ACKNOWLEDGEMENTS.....</b>	<b>80</b>



## PROLOGUE

*“The competitive advantage that the United States military has long enjoyed is eroding... In just a few years, if we do not change the trajectory, we will lose our qualitative and our quantitative competitive advantage. The consequences will be profound.”<sup>1</sup>*

—Gen. Joseph F. Dunford Jr., Chairman of the Joint Chiefs of Staff, June 2017

The United States faces an array of threats to our national security that is nearly unprecedented in its breadth and pace of change. Great power competition from Russia and China, which are both rapidly advancing next-generation warfighting capabilities to leapfrog our legacy systems, presents a dual threat unseen since the military surge of Axis Powers in the 1930s. At the same time, the threat of transnational terrorism that has been the focus of the Department of Defense for the last two decades persists, exacerbated by levels of migration unseen since World War II, the organizing power of social media, and the mounting pressures of climate change.

At home, America faces historic levels of social and political division that makes consensus around budgets, priorities, and a realistic evaluation of our national security threats particularly difficult. All this demands a re-examination of the Department of Defense’s strategy to ensure that its budgetary and policy priorities—as mandated by Congress—are focused on the needs of the future and not on the political and military-industrial loyalties of the past.

This has been the mission of the Future of Defense Task Force: to evaluate the strategic priorities of the U.S. Department of Defense in order to better match national resources to next-generation threats. Our goal has been to create a roadmap for the national security community for the next 30 to 50 years. Our investigation quickly revealed, however, that a whole-of-nation approach would be necessary for its implementation and success, so in that vein, this report is also a letter to the American people.

The stakes could scarcely be higher. The national security challenges the United States faces today are existential, and they cannot be met by simply doubling down on old models of policy and investment. Our adversaries are surging around the globe in a long-game effort to supplant western-style democracy with a form of authoritarianism that cloaks itself in capitalism as it undermines personal liberties and freedoms. The United States must recognize that without a new commitment to achieving technological superiority, the successes of the 20<sup>th</sup> century—the American Century—will no longer be assured.

Historically, the United States has risen to the challenge: the Marshall Plan, the development of the polio vaccine, and the Mercury and Apollo space programs are but a few examples of American ingenuity and leadership in the face of adversity. We are in a 21<sup>st</sup> century moment, and we

<sup>1</sup> Senate Armed Services Committee, *Testimony of Chairman of the Joint Chiefs Gen. Joseph F. Dunford Jr., Hearing to Receive Testimony on the Department of Defense Budget Posture in Review of the Defense Authorization Request for Fiscal Year 2018 and the Future Years Defense Program*. (June 13, 2017) (online at [https://www.armed-services.senate.gov/imo/media/doc/17-58\\_06-13-17.pdf](https://www.armed-services.senate.gov/imo/media/doc/17-58_06-13-17.pdf)).

believe the United States can meet it resoundingly. Ensuring the future of our defense is essential to ensuring the future of our peace. But it will take some serious work. This report does not anticipate how this conversation concludes, but rather lays out how it must begin. Where we go with it is up to Congress and the American people.

A handwritten signature in black ink, appearing to read "Seth Moulton".

Seth Moulton  
Chair

A handwritten signature in black ink, appearing to read "Jim Banks".

Jim Banks  
Chair



## **TASK FORCE CHAIRS**

**CHAIR SETH MOULTON**  
(D-MASS.)

**CHAIR JIM BANKS**  
(R-IND.)

## **TASK FORCE MEMBERS**

**SUSAN DAVIS**  
(D-CALIF.)

**SCOTT DESJARLAIS**  
(R-TENN.)

**CHRISSY HOULAHAN**  
(D-PA.)

**PAUL MITCHELL**  
(R-MICH.)

**ELISSA SLOTKIN**  
(D-MICH.)

**MICHAEL WALTZ**  
(R-FLA.)



## FINDINGS

- I. China represents the most significant economic and national security threat to the United States over the next 20 to 30 years. Because of its nuclear arsenal and ongoing efforts to undermine Western democratic governments, Russia presents the most immediate threat to the United States; however, Russia's long-term economic forecast makes its global power likely to recede over the next 20 to 30 years.
- II. As a result of historic levels of government-sponsored science and technology research, and the inherent advantages of a free market economy, the United States emerged from the Cold War with a substantial economic and military lead over any potential rival. However, these gaps have dramatically narrowed. China will soon overtake the United States as the world's largest economy, and despite historic defense budgets, the United States has failed to keep pace with China's and Russia's military modernization.
- III. Assuring the United States' continued leadership will require dramatic changes to the structure and implementation of the defense budget, the effective implementation of a whole-of-government approach to security, and the strengthening of underlying institutions such as our education system and national security innovation base to out-pace our adversaries.
- IV. Advancements in artificial intelligence, biotechnology, quantum computing, and space, cyber, and electronic warfare, among others, are making traditional battlefields and boundaries increasingly irrelevant. To remain competitive, the United States must prioritize the development of emerging technologies over fielding and maintaining legacy systems. This will require significant changes to the Pentagon's force structure, posture, operational plans, and acquisition system and must be complemented by a tough and fulsome review of legacy systems, platforms, and missions.
- V. The Pentagon's emerging operational concepts have the potential to provide the U.S. military a decisive advantage, but they are not yet fully viable. To address current and future threats and deter conflict, the Department of Defense must more aggressively test new operational concepts against emerging technologies.
- VI. To endure as the leading global power with preeminent economic might, political influence, and a resilient national security apparatus, the United States must strengthen and modernize geopolitical alliances with longstanding allies while establishing new alliances to meet emerging threats.
- VII. Technological advancements in artificial intelligence and biotechnology will have an outsized impact on national security; the potential of losing this race to China carries significant economic, political, and ethical risks for the United States and our free democratic allies for decades to come. Winning this race requires a whole-of-nation approach where the distinct advantages of both America's private and public sector are harnessed and synthesized.

- VIII. Increased government investment in basic scientific research must be complemented by increased cooperation with the private sector to quickly adopt resulting technologies. The Department of Defense and elements of the greater U.S. government must adapt their culture and business practices to better support, and more quickly integrate, innovation from the private sector.
- IX. Whereas emerging technologies offer tremendous opportunities for commercial and social transformation, many are also fraught with the potential for nefarious use. It is essential that the United States and our free democratic allies set and enforce the terms and norms for their employment.
- X. Authoritarianism is on the rise globally, whereas democracy is waning. A whole-of-government approach to national security should be led by diplomacy and economic cooperation, supported by development and humanitarian assistance, and strengthened by military-to-military relationships.
- XI. The United States is most likely to succeed by playing to our strengths: a free, fair, and open economy, strong education system, and a culture for innovation that rests on the open market and free democratic principles.

## RECOMMENDATIONS

- I. Using the Manhattan Project as a model, the United States must undertake and win the artificial intelligence race by leading in the invention and deployment of AI while establishing the standards for its public and private use. Although the Department of Defense has increased investment in AI and established the Joint Artificial Intelligence Center to assist with the transition and deployment of AI capabilities, cultural resistance to its wider adoption remains. Congress and the Department of Defense must take additional action to overcome these barriers.
  - a. Require every Major Defense Acquisition Program to evaluate at least one AI or autonomous alternative prior to funding.
  - b. Require all new Major Defense Acquisition Programs to be AI-ready and nest with existing and planned joint all-domain command and control networks.
  - c. Expand the Department of Defense's authorities and abilities to evaluate high technology readiness level items and technologies that satisfy defense requirements to reduce risk for major acquisition programs, lower procurement costs, and accelerate the fielding of critical capabilities.
- II. Because of the United States' commitment to human rights, and to ensure those rights are enshrined in its use, the United States should lead in the formulation and ratification of a global treaty on artificial intelligence in the vein of the Geneva Conventions, the Chemical Weapons Convention, and the Nuclear Non-Proliferation Treaty to establish guardrails and protections for the civilian and military use of AI.
  - a. Nations that adhere to democratic principles should lead in the creation of the global treaty, which would establish accountability, promote collaboration and transparency, ensure fairness, and limit the harmful use of AI.
  - b. The treaty should further establish an international code of ethics and privacy protections that ensure personal freedoms and liberties globally.
  - c. The document must be amendable to allow for advancements in technology.
  - d. The stated goal must be for all nations, especially those that are developing and employing AI, to be included as signatories.
- III. The United States must ensure supply chain resiliency within both the military and civilian sectors by establishing reliable manufacturing sources and incentivizing the return of manufacturing to the homeland through fiscal policy, tax incentives, and other financial and policy measures.
  - a. Form a National Supply Chain Intelligence Center under the Director of National Intelligence to monitor and protect U.S. supply chain interests.
  - b. Identify and eliminate single points of failure within the Department of Defense supply chain.
  - c. Bolster and expand the Information and Communications Technology Supply Chain Risk Management Task Force within the Department of Homeland Security to identify and secure the civilian supply chain equities that affect U.S. national security interests.

- d. Strengthen the Committee on Foreign Investment in the United States (CFIUS) and the Foreign Investment Risk Review Modernization Act (FIRRMA) regulations to include additional industries relevant to AI, quantum computing, sensing, autonomy, space, and robotics.
- IV. To compete against 21<sup>st</sup> century adversaries, Congress and the Department of Defense must identify, replace, and retire costly and ineffective legacy platforms. The Task Force recommends that Congress commission the RAND Corporation (or similar entity) and the Government Accountability Office to study legacy platforms within the Department of Defense and determine their relevance and resiliency to emerging threats over the next 50 years.
- a. The studies should survey all services, agencies and entities within the Department of Defense to include hardware, weapons systems, basing, and force structure.
  - b. With an emphasis on agility, technology, and an expanded forward foot print, studies should make recommendations for future force structure and investment.
  - c. Following completion of the studies, a panel should be convened, comprising Congress, the Department of Defense, and representatives from the industrial base to make recommendations on which platforms should be retired, replaced or recapitalized.
- V. The U.S. homeland remains uniquely vulnerable to adversaries who are increasing their ability to wage cyberwarfare against civilian populations through attacks on infrastructure, financial institutions, and healthcare facilities, among others. The United States should prioritize cyber-attack and gray zone defense capabilities within both the Department of Defense and the private sector.
- a. Examine the relationship between executive branch departments and agencies with independent regulatory agencies overseeing critical infrastructure sectors to ensure that information related to cybersecurity is shared by default, rather than by exception.
  - b. Create parity between the defense industrial base and other critical infrastructure sectors by establishing an independent regulatory agency to define and enforce threat-informed cybersecurity standards through regular assessments of defense contractors. Ensure robust enforcement mechanisms to include the authority to levy financial penalties against non-compliant defense contractors.
  - c. Bolster the partnership between U.S. Cyber Command and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, notably the operational partnership in national defense and incident response.
  - d. Develop tactical cyber operational forces within all military services to integrate them into conventional kinetic operations to foster interoperability between conventional operational activities and cyberspace activities.
  - e. Recognizing that many of the Pentagon's major weapon systems are vulnerable to cyber intrusion and disruption, the Department of Defense must recruit and foster a technologically astute workforce that can develop and procure the requisite capability to mitigate potential vulnerabilities.
  - f. Create tax and other financial incentives for the private sector to invest in cybersecurity and prepare for gray zone attacks.

- VI. Because an engaged and informed electorate is essential for a republic to endure, the United States should expand voluntary National Service programs. Promoting volunteerism and active engagement in democracy bolsters our national security through participation and shared experiences.
- a. Integrate military, national, and public service to create interoperability within these sectors.
  - b. Initiate paid, year-of-service programs with civilian, military, and private-sector pathways for youth.
  - c. Incentivize service through student loan deferment and forgiveness.
  - d. Create mentorship and apprentice opportunities within National Service programs.
  - e. Encourage civics and personal citizenship curricula in public schools.
- VII. To maintain its global preeminence in scientific and technological innovation and the associated economic and military advantage, the United States should increase its investment in foundational science and technology research by committing to spending at least one percent of the country's gross domestic product on basic government-supported research and development.
- a. The Pentagon should increase funding for science and technology research programs to meet the 3.4 percent of the overall defense budget recommended by the Defense Science Board.
  - b. Expand funding for historically successful innovation efforts such as Defense Advanced Research Projects Agency, the national and defense research laboratories, and university partnerships.
  - c. Require the military services to spend at least one percent of their overall budgets on the integration of new technologies.
  - d. Establish target funding levels with defense allies for investment in science and technology research.
- VIII. To maintain its technological advantage over competitors, the Pentagon must continue to improve its ability to leverage private sector innovation at scale, including that from non-traditional companies, recognizing that the private sector, not the government, is now the leader in research and development investment.
- a. Increase funding for successful innovation efforts such as the Defense Innovation Unit, AFWERX, Army Futures Command, and others that successfully bridge the gap between innovative organizations and the military ten-fold, and robustly fund established drivers of innovation within the Department of Defense.
  - b. Restore the Department of Defense Rapid Innovation Fund, which was authorized in FY11, to assess, fund, and accelerate innovative technology solutions for the warfighter. This fund is a critical pathway for relevant late-stage technologies to be funded inside the Department of Defense.
  - c. Create additional opportunities for collaboration and shared experience between the Department of Defense, private sector, and academia through the expansion of programs such as Hacking for Defense and partnerships with groups such as the Silicon Valley Defense Working Group.

- IX. To sustain the world order that has allowed the United States to prosper and thrive for more than 70 years, the United States must foster new and creative partnerships for a changing world while strengthening existing alliances and security agreements. Such engagements will further vital U.S. national security interests by ensuring placement, access, resiliency and redundancy while creating complex problem sets for adversaries.
- a. Enhance essential partnerships with North Atlantic Treaty Organization and Five-Eyes intelligence partners, Canada, United Kingdom, Australia, and New Zealand—as well as with Japan and South Korea.
  - b. Develop a modern Western Hemisphere policy that protects U.S. Latin and Central American interests and alliances while simultaneously expanding a robust Arctic Strategy.
  - c. Bolster ties with allies in the Middle East, notably Israel and Jordan.
  - d. Strengthen relations with longstanding Asian security partners such as Thailand, the Philippines, Taiwan, and Singapore while growing relationships with India, Vietnam, Indonesia and Malaysia, among others.
  - e. Cultivate economic and diplomatic cooperation with non-traditional allies, especially in Asia and Africa.
  - f. Increase foreign military sales with security partners and bolster the International Military Education and Training program following enhanced vetting.
  - g. Extend New START and negotiate a follow-on agreement.
- X. Recognizing that human capital is our most important asset, the United States should increase its investment in science, technology, engineering, and mathematics within the Department of Defense and foster STEM talent through a whole-of-government approach to ensure the nation's scientific and technological advantage in the public and private sectors endures.
- a. Invest in STEM primary education.
  - b. Attract and retain foreign STEM talent to study and work in the United States through specialized visas and scholarships. Support H.R. 7256, the National Security Innovation Pathway Act, which provides a mechanism to retain U.S.-educated experts to continue working in the defense innovation base on critical technologies, and H.R. 6526, the STEM Corps Act, which enhances STEM and computer science within the Department of Defense workforce.
  - c. Improve hiring pathways and increase compensation for STEM careers at the Pentagon and in the private sector; create a military commissioning source for STEM talent.
  - d. Streamline security clearances by beginning the vetting process in graduate school.
  - e. Build STEM incentives into the service academies through scholarships and curricula.
  - f. Enable and incentivize “Tour of Duty” opportunities for private sector technical talent to serve tours within the Department of Defense.
- XI. To maintain the United States' military advantage against emerging threats, the Pentagon must refine its operational concepts by employing new technologies and methods to deter future conflicts and compete in the gray zone of hybrid warfare.
- a. The Pentagon, Congress, and the Intelligence Community should work in tandem to identify trends and threats 10 to 30 years beyond the normal budget cycle while



expanding entities within their respective organizations to incorporate long-term planning.

- b. The Department of Defense should adhere to a whole-of-government approach and work with other departments such as State and Treasury to develop and execute a comprehensive strategy to compete in the gray zone.
- c. Create a task force to ensure a diverse group of stakeholders, including Congress, academia, think tanks, and the private sector are engaged in developing imaginative solutions to emerging military challenges and in assessing the Pentagon's efforts.
- d. Increase funding for wargaming and large-force joint exercises to assess new operational concepts; increase prototyping and testing with the emerging technologies needed to underpin these concepts.
- e. Prioritize the development and procurement of critical capabilities for future conflict models such as resilient command and control networks, logistics capabilities and the defense of forward and expeditionary basing.
- f. Invest in programs of record to directly support emerging operational concepts.

XII. The United States is operating under an authorization for the use of military force that is nearly two decades old. Emerging threat streams require the United States to make strategic choices and prioritize its military actions. Congress must uphold its constitutional obligation to determine how and where the United States employs its military force by passing an updated AUMF.

- a. Congress should reaffirm its constitutional obligation by evaluating the nation's national security objectives and military strategy by passing an updated AUMF.
- b. Revising the AUMF ensures that the United States can operate in a dynamic threat environment while signaling to both allies and adversaries that America is committed to the lawful pursuit of its military endeavors.

XIII. To incorporate the technology necessary to maintain the United States' military supremacy, the Pentagon must continue refining its acquisition process to be more agile and less risk-averse so that it can fully leverage emerging technologies and capabilities at scale.

- a. Review defense acquisition regulations to make them less onerous, particularly for non-traditional entities seeking to partner with the Department of Defense.
- b. Train and incentivize the acquisition workforce to utilize existing flexible authorities to quickly push innovative technology to warfighters in the field.
- c. Incentivize calculated risk by providing funding for emerging technologies through programs of record at scale; allow a less-than-perfect success rate.
- d. Significantly increase opportunities for operators in the field, the acquisition force, program managers, and industry to partner and work together to more quickly develop requirements and identify solutions.
- e. Structure the acquisition process, particularly for programs heavily dependent on software and technology, to be continuous and more closely aligned with the iterative process used to develop software and emerging technologies.
- f. Employ the Air Force "Kessel Run" model, which works directly with operational units for rapid development and field testing.

XIV. To thwart emerging threats and compete with adversaries who seek to undermine the United States beyond military realms to include economic, information, and political domains, the nation should reconfigure a coordinated, whole-of-government strategy to update the

national security structure, which was established in the 1940's primarily to focus on the rise of communism. This reimagination of the national security structure would partner the Department of State with the Department of Defense to ensure diplomatic parity and leadership.

- a. The State Department should lead the nation's whole-of-government effort, and its funding and staffing should be exponentially increased to reflect its expanded role and prominence. Congress should allocate funding to hire additional foreign service officers and expand the Global Engagement Center to counter foreign propaganda and misinformation.
- b. Congress should commission a varied group of national security experts and practitioners to undertake a wide-ranging review of the national security structure and strategy for adapting and restructuring them to incorporate new technologies and operational concepts and thus compete in the 21st Century.

## EXECUTIVE SUMMARY

The gravity and complexity of threats emerging to challenge the United States is proliferating as technological advancements in artificial intelligence, quantum information science, and biotechnology transform society and weaponry at an exponential rate. This is occurring as adversarial capability is increasing to the point where the United States may soon lose the competitive military advantage it has enjoyed for decades.<sup>1</sup>

The free world order the U.S. has led for more than 70 years is now in danger of becoming a historical outlier as an alternate form of authoritarianism, one that seeks to emulate capitalism and supplant western-style democracy as the governing standard, is on the rise.

To remain economically and militarily competitive, and to ensure American leadership into the next century, policy makers and the Pentagon must navigate a major course correction in how we invest in national security. This will require a paradigm shift in our defense posture from heavy, expensive, and antiquated, to lean, adaptive, and integrated.

This strategy will require a whole-of-nation approach, one that embraces emerging technologies, aggressively divests of aging and expensive platforms, and more effectively harnesses ingenuity and innovation from the private sector.

The Future of Defense Task Force was established to investigate and assess how to address these challenges. Our findings and recommendations are intended as a roadmap for the greater national security community, and whereas our report should be considered a white paper, it builds upon the extensive work of the House Armed Services Committee, Department of Defense, military services, private industry, think tanks, and academia.

This report is neither exhaustive nor conclusive; rather, it is the beginning of a difficult yet necessary conversation. Congress and the American people must recognize that we face a decisive moment as a nation and as the world's leading democracy, both of which are in peril until we alter the future of our defense to ensure the future of our peace.

### Emerging Threats

A complex and evolving array of national security threats are facing the United States, as its political, economic, and military rivals are increasing in stature and capability. Rising powers, notably China and Russia, threaten to cause tectonic shifts in geopolitical plates where, much like the Cold

<sup>1</sup> Senate Armed Services Committee, *Testimony of Chairman of the Joint Chiefs Gen. Joseph F. Dunford Jr., Hearing to Receive Testimony on the Department of Defense Budget Posture in Review of the Defense Authorization Request for Fiscal Year 2018 and the Future Years Defense Program*. (June 13, 2017) (online at [https://www.armed-services.senate.gov/imo/media/doc/17-58\\_06-13-17.pdf](https://www.armed-services.senate.gov/imo/media/doc/17-58_06-13-17.pdf)).

War, the binary notions of war and peace are becoming antiquated. Future conflicts will be increasingly waged in the gray zone, the nebulous battlespace below open combat, where tactics such as economic coercion, cyber espionage, disinformation, and unattributed military forces are employed.

Adding to the complexity is the recognition that the nature of warfare is evolving with the weaponization of emerging technologies that changes the way wars are fought and won. The rapidly expanding domains of space and cyberspace are the new frontiers for conflict and will be the battlefield of choice for the opening salvo of any aggressor.

Climate change, determined by the Department of Defense to be a threat multiplier,<sup>2</sup> is generating widespread upheaval owing to cataclysmic events such as wildfires, drought, and flooding while further increasing the global competition for resources.

A provocative Iran is lashing out in the Middle East, while North Korea continues its march toward full nuclearization. Terrorism, waged by violent extremist organizations, continues to threaten vital U.S. partners and interests in Europe, the Middle East, and Africa, while transnational criminal organizations wreak havoc on vulnerable populations. Divisive politics and a disparate electorate in the homeland further threaten U.S. national security.

## **The Weaponization of Emerging Technology**

A sophisticated array of emerging technologies and new weaponry, in various stages of development, will fundamentally change the nature of conflict along with the very battlespace where it will be fought. The stakes are high. Whoever achieves superiority in this technological race will enjoy significant military and economic advantage for decades—and possibly into the next century. Achieving this supremacy will require a whole-of-nation approach, where the distinct advantages of both the private and public sector are harnessed and synthesized.

Whereas many of these technologies offer tremendous opportunity for commercial and social transformation, they are also rife with the potential for nefarious use and may exponentially exacerbate threat streams for the U.S. and its global partners.

Advancements in artificial intelligence, quantum information science, space and cyber and electronic warfare, among others, are making traditional battlefields and boundaries increasingly irrelevant. To remain competitive, the U.S. must recognize this shift and prioritize the development of emerging technologies while also increasing its ability to defend against them.

Technology is pulling warfare into a post-conventional era, wherein the first hours of conflict will no longer be saturated with aerial bombings and sea landings followed by a ground assault. Initial campaigns will be fought with remote and autonomous systems in the realms of space and cyberspace, where an early attack will take out satellite and communication systems and dismantle the global positioning system (GPS). Opening salvos could inflict devastating harm on

<sup>2</sup> Department of Defense, *Report on the Effects of Climate Change* (Jan. 10, 2019) (online at <https://media.defense.gov/2019/Jan/29/2002084200/-1/-1/1/CLIMATE-CHANGE-REPORT-2019.PDF>).

civilians through electronic attacks on critical infrastructure and power grids, along with financial and healthcare systems and networks.

Also, while most of the technologies will require substantial funding and development by state actors, others such as cyber and electronic warfare may allow less formidable foes to gain the operational upper hand with limited investment. Therefore, as adversaries build and recapitalize conventional and strategic weapons, a parallel effort will be underway to develop systems that adhere to the David and Goliath paradigm: instead of taking on the giant pound for pound, build nimble and inexpensive sling shots.

It is essential for the U.S. to increase its ability to defend against adversaries who will seek early domination in a conflict by disrupting and degrading both civilian and military systems and networks. The disruption of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) has become a bedrock operational concept of 21<sup>st</sup> century warfare.<sup>3</sup> The ability of the U.S. to leverage offensive and defensive capabilities in this realm is paramount to maintaining the global balance of power as well as strategic and conventional military superiority.

## **Partners and Security Alliances**

To secure vital national security interests at home and abroad, the U.S. should strengthen its existing security alliances while working to build new ones. Engaging global partners through diplomacy, economics, humanitarian aid, security cooperation, and military-to-military relations is among the most notable actions the U.S. can take to ensure continued peace, financial stability, and strategic advantage when gaming out the future of defense.

To endure as a global democratic power with economic and political influence and a resilient forward military footprint, the U.S. must strengthen its geopolitical alliances with longstanding allies while fostering relationships with new partners. Maintaining robust ties with its Five Eyes intelligence partners—Canada, United Kingdom, Australia, and New Zealand—as well as with the North Atlantic Treaty Association is essential. Equally important are relationships with Japan and South Korea.

Key allies in the Middle East, notably Israel and Jordan, among others, will continue to be vital U.S. partners. The U.S. should also cultivate economic and diplomatic cooperation with non-traditional allies in Asia and Africa while re-engaging in the Western Hemisphere with both Latin American and Arctic partners.

<sup>3</sup> Michele Flournoy and Gabrielle Chefetz, *Sharpening the U.S. Military's Edge: Critical Steps for the Next Administration*, Center for a New American Security (July 13, 2020) (online at [https://www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration?utm\\_medium=email&utm\\_campaign=Defense+Launch+of+Next+Defense+Strategy+Project+press+release&utm\\_content=Defense+Launch+of+Next+Defense+Strategy+Project+press+release+CID\\_c709fecb79ba4caf85b2cc0ae4632700&utm\\_source=Campaign+Monitor&utm\\_term=Sharpening+the+US+Militarys+Edge+Critical+Steps+for+the+Next+Administration](https://www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration?utm_medium=email&utm_campaign=Defense+Launch+of+Next+Defense+Strategy+Project+press+release&utm_content=Defense+Launch+of+Next+Defense+Strategy+Project+press+release+CID_c709fecb79ba4caf85b2cc0ae4632700&utm_source=Campaign+Monitor&utm_term=Sharpening+the+US+Militarys+Edge+Critical+Steps+for+the+Next+Administration)).

Strong offensive measures in the form of soft power initiatives protect vital U.S. interests by ensuring dialogue and enhanced cooperation. Humanitarian and economic aid programs foster good will and build civic capacity while also serving as a powerful check on the rise of authoritarian and autocratic influence. Exporting democracy through American projects and enterprises showcases democratic values such as human rights, personal liberties, and self-determination.

The U.S. military, with its adherence to human rights and the rules of engagement, stands as the global model for how a free and open society should protect itself and its interests. Exporting U.S. values through military engagements, with both exercises and train and assist programs, builds trust and interoperability while increasing readiness and resiliency and further protecting vital U.S. interests abroad. Strengthening global partnerships through military-to-military relations allows the U.S. to maintain an agile forward footprint while bolstering the doctrine of credible deterrence.<sup>4</sup>

Longstanding bilateral security agreements with Japan and South Korea, which hold considerable historical agency, also serve as prescient alliances in the wake of a rising China. Moreover, the U.S. and Russia should extend the highly successful Strategic Arms Reduction Treaty (New START) while negotiating a follow-on agreement.<sup>5</sup>

When gaming out the future of defense, the increasingly strained relations with China and the rising potential for conflict with Russia should remind the U.S. to consider diplomatic measures that adhere to the concept of statecraft versus the proliferation of war craft. Leveraging influence through economic, political, and social measures may be the most successful means of avoiding conflict while ensuring a stable, open, and transparent world order that allows democracies to thrive.

## **Supercharging the Innovation Base**

The U.S. has long been the global leader in technological innovation because of its investment in government-funded research and development (R&D) that has led to breakthroughs such as the Manhattan Project and the space program. Without increased investment and focus, however, its pre-eminence is at risk.

Historically, the U.S. has outpaced every other country in overall R&D spending, but its lead is quickly diminishing. Over the past two decades, China has rapidly increased its investment in overall R&D, whereas U.S. spending rates have lagged. Today, the U.S. still spends more than any other country, but China is on track to take the lead in global R&D spending by 2030 if current trends continue.<sup>6</sup>

Defense funding for science and technology programs, which have cultivated game-changing dual-use capabilities such as GPS and the Internet, has barely kept pace with inflation, as the military

<sup>4</sup> House Armed Services Committee, Testimony of Michele Flournoy, *Theories of Victory-Innovative Concepts for National Security* (Oct. 29, 2019) (online at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventId=110154>).

<sup>5</sup> Brian Sittlow, *New START: The Future of U.S.-Russian Arms Control*, Council on Foreign Relations (Jan. 28, 2020) (online at <https://www.cfr.org/in-brief/new-start-future-us-russia-nuclear-arms-control>).

<sup>6</sup> Council on Foreign Relations, *Innovation and National Security: Keeping Our Edge* (2019) (online at [https://www.cfr.org/report/keeping-our-edge/pdf/TFR\\_Innovation\\_Strategy.pdf](https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf)).

focuses on shorter term and incremental developments. While it is now the private sector, rather than the government, who is the primary funder of scientific R&D globally, private funding cannot replace the type of long-term basic R&D funding that has long-afforded the U.S. economic and military advantage. Also, because the private sector has a different incentive structure, no single company can match the federal government's size and investment.

The Pentagon must harness private sector technology and innovation at scale to maintain its technological advantage by supporting proven drivers of innovation such as the Defense Advanced Research Projects Agency (DARPA) and the defense research laboratories while fostering new initiatives such as the Defense Innovation Unit (DIU) and Army Futures Command. Most importantly, it must commit to investing in new innovative capabilities at scale by making them programs of record.

The U.S. should also re-establish its domestic manufacturing and supply chain capability, which is both an economic driver and a national security imperative. As the COVID-19 pandemic has illustrated, a lack of domestic manufacturing capability and access to reliable supply chains is among our greatest national security and economic vulnerabilities.

## **Developing a 21st Century Workforce**

Science, technology, engineering, and mathematics (STEM) talent and education are the fundamental building blocks of the technological innovation necessary to maintain the U.S.'s strategic advantage. While the U.S. has long had an advantage owing to its investment in STEM education, its pre-eminence is at risk, as global competitors rush to catch up. To maintain its lead, the U.S. must grow talent at home and aggressively recruit it from abroad.

The quantifiable success of recent immigrants to the U.S. is staggering. Nearly half of all Fortune 500 companies in the U.S., valued collectively at \$5.3 trillion in 2017, were started by first- or second-generation Americans.<sup>7</sup> According to the National Science Foundation, 72 percent of foreign doctoral students were still in the U.S. 10 years after earning their degrees, including 90 percent of Chinese students.<sup>8</sup>

Still, immigration policy hinders the U.S.'s ability to attract and retain foreign STEM talent that instead flows to other countries, including competitors. This occurs even as American companies, many from the military industrial base, have asserted they need additional STEM talent from abroad.<sup>9</sup>

To maintain its competitive advantage, the U.S. must also modernize its personnel system to recruit, retain, and promote military talent. The changing nature of warfare dictates that the modern U.S. military will need an increasing number of service members capable of operating in a complex

<sup>7</sup> Ian Hatchway, *Almost half of Fortune 500 Companies were founded by American immigrants or their children*, Brookings Institution (Dec. 2017) (online at <https://www.brookings.edu/blog/the-avenue/2017/12/04/almost-half-of-fortune-500-companies-were-founded-by-american-immigrants-or-their-children/>).

<sup>8</sup> Congressional Research Service, *Foreign STEM Students in the United States* (Nov. 1, 2019) (online at <https://crsreports.congress.gov/product/pdf/IF/IF11347>).

<sup>9</sup> Council on Foreign Relations, *Innovation and National Security: Keeping Our Edge* (2019) (online at [https://www.cfr.org/report/keeping-our-edge/pdf/TFR\\_Innovation\\_Strategy.pdf](https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf)).

and fast-moving battlespace with limited communication or direction from higher authority. In addition to combat leadership skills, the military must attract and promote service members with the intellectual acumen to develop the strategic and operational concepts necessary to deter conflict and be competitive in the future.

Although the U.S. military personnel system produces outstanding leaders, it must grow its ability to produce more service members with expanded capabilities to meet emerging threats. History repeatedly shows that technological superiority does not guarantee victory and that new ways of thinking can be more powerful than new weapons. Future leaders and strategists will need to embrace emerging warfighting concepts such as joint and multi-domain warfare. They will further need a comprehensive understanding of national power and how to integrate military tools into a whole-of-government effort.

A strong civilian national security workforce is an equally critical component of the U.S.'s strategic and military advantage. Like the military, it will need to update its personnel system to attract and retain a diverse group of workers with the critical skills necessary to remain competitive in evolving defense apparatuses.

## **Financial Trade-Offs and Acquisition Reform**

U.S. federal budgets are expected to contract in the near term, even as national security threats become increasingly complex and powerful. Simultaneously, critical domestic needs will compete with defense spending for limited resources. As this tension unfolds, the U.S. faces a dynamic array of challenges, many of which cannot be solved through traditional defense spending. This new paradigm will require a broad view of what investments are considered critical to the nation's security as well as hard choices about how to apportion increasingly limited resources.

Policy makers, industry, and the Pentagon must work together to identify trade-offs within the defense apparatus to include legacy systems and operations, which will allow for investment in technology and operational concepts to address future challenges. The Pentagon will further need to refine its acquisition process and improve its ability to incorporate innovative emerging technologies and capabilities at the scale required to succeed in an era of great power competition.

China's economic power continues to grow, and China remains on a glide path to be the world's largest economy by as early as 2030.<sup>10</sup> If the U.S. defense posture maintains its current trajectory, 70 percent of the military's systems will be legacy platforms when that occurs.<sup>11</sup> In contrast, China and Russia adhere to fewer traditional systems, allowing them to more easily field future capabilities.

<sup>10</sup> Michael Brown, Eric Chewning, Pavneet Singh, *Preparing the United States for the Superpower Marathon with China*, The Brookings Institution (April 2020) (online at <https://www.brookings.edu/research/preparing-the-united-states-for-the-superpower-marathon-with-china/>).

<sup>11</sup> Michele Flournoy and Gabrielle Chefetz, *Sharpening the U.S. Military's Edge: Critical Steps for the Next Administration*, Center for New American Security (July 13, 2020) (online at <https://www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration>).



To meet these challenges and fully incorporate the critical emerging technologies they need, the Pentagon must make its acquisition process more agile, creative, and less risk-averse. The current system is predisposed and incentivized to invest in incrementally better versions of existing legacy systems; instead, it should incorporate new technology that will underpin innovative operational concepts.

The Pentagon must also work with Congress to identify innovative capabilities and ensure that the acquisition process is finely tuned to make substantial investments to procure them at the necessary scale. Such programs, identified to support new operational concepts, should then be fast-tracked to avoid the “valley of death,” where, too often, initiatives fail to become funded programs of record.

## **Operational Concepts**

The military is developing game-changing operational concepts to leverage new innovative technology and thinking; however, it has yet to fully procure the systems and capacity necessary to fully implement these initiatives. Therefore, the Pentagon must enhance its capability, expertise, and processes to rigorously define military challenges while also designing and correlating programs of record and incorporating them into new operational concepts.

To that end, the military must work with Congress to connect its investments to key priorities in support of operational concepts. It should engage a diverse group of stakeholders, including Congress, academia, think tanks, and the private sector, to develop imaginative solutions to emerging problems while assessing the Pentagon’s efforts.<sup>12</sup> It is further essential to test, experiment, and wargame new operational concepts and to prototype and test the technologies that underpin them.

The most effective military operational concepts and associated military capacity, however, will still be insufficient to address the breadth of the challenges posed by strategic competitors. A whole-of-nation effort, including military tools, trade policy, STEM education, diplomatic initiatives, and non-military instruments, is necessary to meet these emerging threats. Without this approach, the U.S. will not be postured to maintain its security and global influence, even if the military is robustly equipped and funded. The problem sets competitors present are comprehensive, and the nation’s response must be equally broad.<sup>13</sup>

New strategies must effectively dissuade competitors from challenging the U.S. in the gray zone with weapons of economic coercion and information warfare. Conventionally, the U.S. military is no longer assured the complete dominance in air, sea, and space it has enjoyed for decades, as adversaries prioritize weapon systems such as long-range munitions, anti-space capabilities, and cyber forces.

<sup>12</sup> National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Nov. 2018) (online at <https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf>).

<sup>13</sup> National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Nov. 2018) (online at <https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf>).

According to the latest Department of Defense assessment, China has doubled its defense spending in the last decade and now has more ships than the U.S. Navy, among the best air defense systems globally, an arsenal of long-range ballistic missiles, and a variety of other means to challenge the U.S.<sup>14</sup> A sobering report from the RAND Corporation recently determined that despite significantly outspending China and Russia, the U.S. military could lose a future conflict because it failed to adequately posture and train.<sup>15</sup>

New operational concepts must be devised and employed to meet these challenges by leveraging emerging technologies across multi-domains to ensure the U.S. maintains both credible deterrence and strategic advantage.

<sup>14</sup> Department of Defense, *Military and Security Developments Involving the People's Republic of China* (2020) (online at <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>).

<sup>15</sup> David Ochmanek, Peter Wilson, Brenna Allen, John Speed Meyers, Carter Price, *U.S. Military Capabilities and Forces for a Dangerous World*, RAND Corporation (2017) (online at [https://www.rand.org/pubs/research\\_reports/RR1782-1.html](https://www.rand.org/pubs/research_reports/RR1782-1.html)).

# EVIDENCE

## EMERGING THREAT STREAMS

A complex and evolving array of national security threats are facing the United States as political, economic, and military rivals increase in stature and capability. Rising powers, notably China and Russia, threaten to cause tectonic shifts in geopolitical plates where, much like the Cold War, the binary notions of war and peace are becoming antiquated. Future conflicts will be increasingly waged in the gray zone, the nebulous battlespace below open combat where tactics such as economic coercion, cyber espionage, disinformation, and unattributed military forces are employed.

Adding to the complexity is the recognition that the nature of warfare is changing, as the weaponization of emerging technologies appears poised to change the way wars are fought and won. Indeed, the very concept of victory may be changing along with the notion of what winning looks like. The rapidly evolving domains of space and cyberspace are the new frontiers for conflict and will be the battlefield of choice for the opening salvo of any aggressor.

A provocative Iran is lashing out in the Middle East while North Korea continues its march toward full nuclearization. Terrorism, waged by violent extremist organizations (VEOs), continues to threaten vital U.S. partners and interests in Europe, the Middle East, and Africa while transnational criminal organizations (TNOs) wreak havoc on vulnerable populations. Divisive politics and a disparate electorate in the homeland further threaten U.S. national security. Climate change, determined by the Department of Defense (DOD) to be a threat multiplier,<sup>1</sup> is generating widespread upheaval due to cataclysmic events such as wildfires, drought, and flooding while further increasing the global competition for resources.

### China

During his address to the 19<sup>th</sup> Party Congress in 2017, Chinese President Xi Jinping laid out a roadmap to transform China into a global power within 30 years.<sup>2</sup> Since then, there has been speculation among national security experts that China aspires to supersede the United States as the world's only superpower by 2049, the 100<sup>th</sup> anniversary of its modern founding.<sup>3</sup> Whether it aspires to be a global or regional power, China appears intent on expanding its government model of

<sup>1</sup> Department of Defense, *Report on the Effects of Climate Change* (Jan. 10, 2019) (online at <https://media.defense.gov/2019/Jan/29/2002084200/-1/-1/1/CLIMATE-CHANGE-REPORT-2019.PDF>).

<sup>2</sup> Department of Defense Annual Report to Congress, *Military and Security Developments Involving the People's Republic of China* (May 2, 2019) (online at [https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019\\_CHINA\\_MILITARY\\_POWER\\_REPORT.pdf](https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf)).

<sup>3</sup> Parag Khanna, *China Couldn't Dominate Asia if It Wanted To*, *Foreign Policy* (Feb. 3, 2019) (online at <https://foreignpolicy.com/2019/02/03/china-couldnt-dominate-asia-if-it-wanted-to/>).

authoritarian-style leadership, with a diminished emphasis on human rights and bereft of western tenants such as personal liberty and self-determination.

Currently, the People's Liberation Army is the largest military force in the world, and China is rapidly modernizing its conventional and strategic arsenals while expanding its military footprint globally.<sup>4</sup> Through its military-civil fusion doctrine, China is able to employ a whole-of-nation approach to integrate commercial advancements into its defense apparatus, notably in emerging technologies such as artificial intelligence (AI) and biotechnology.<sup>5</sup> There is consensus among national security experts that China is increasing its ability to compete so rapidly that that it could overtake the United States in military capability in as few as five years.<sup>6</sup>

In 2017, China opened its first foreign military base in Djibouti and is currently planning potential bases in Central and South Asia, the Middle East, and the Western Pacific.<sup>7</sup> In the near term, China is orienting itself as a regional hegemon and has become alarmingly aggressive in the South China Sea where, in a just a few years, it has significantly altered its security footprint by unlawfully militarizing islands, shoals, and atolls in disputed waters.<sup>8</sup> Near Taiwan in the East China Sea, China's territorial assertion over Japan's Senkaku Islands is causing interregional tensions with Japan and South Korea, two of the United States' strongest allies.

Adding to the geopolitical complexity of China's emerging power is the recognition that it is increasing its alliances with authoritarian regimes as it looks to promote its system of authoritarian capitalism as an alternative to democracy.<sup>9</sup>

China's ambitious soft power endeavor, the Belt and Road Initiative, has invested in the economic development of more than 100 countries and made inroads across Asia, Africa, and South America with major infrastructure projects. The massive undertaking has enabled China to increase its political and economic influence globally while laying the groundwork for military expansion.<sup>10</sup> The endeavor has also allowed China significant access to natural resources, critical infrastructure such as ports and airfields, and the ability to continue their dominance in rare earths mining.

China is seeking to set next-generation tech standards, similar to how the United States dominated the last century. In 2017, it announced its "New Generation Artificial Intelligence

<sup>4</sup> Department of Defense, Annual Report to Congress, *Military and Security Developments Involving the People's Republic of China* (May 2, 2019) (online at [https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019\\_CHINA\\_MILITARY\\_POWER\\_REPORT.pdf](https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf)).

<sup>5</sup> Elsa Kania, In Military-Civilian Fusion, *China is Learning Lessons from the United States and Starting to Innovate*, The Strategy Bridge (Aug. 27, 2019) (online at <https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate>).

<sup>6</sup> Kathy Gilsinan, *How the U.S. Could Lose a War with China*, The Atlantic (Jul. 25, 2019) (online at <https://www.theatlantic.com/politics/archive/2019/07/china-us-war/594793/>).

<sup>7</sup> Department of Defense, Annual Report to Congress, *Military and Security Developments Involving the People's Republic of China* (May 2, 2019) (online at [https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019\\_CHINA\\_MILITARY\\_POWER\\_REPORT.pdf](https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf)).

<sup>8</sup> Hannah Beech, *China's Sea Control is a Done Deal Short of War with the U.S.*, New York Times (Sept. 20, 2018) (online at <https://www.nytimes.com/2018/09/20/world/asia/south-china-sea-navy.html>).

<sup>9</sup> Office of the Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (Jan. 29, 2019) (online at <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>).

<sup>10</sup> Andrew Chatzky and James McBride, *China's Massive Belt and Road Initiative*, Council on Foreign Relations (Jan. 28, 2020) (online at <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative>).

Development Plan”<sup>11</sup> and set the ambitious goal of becoming the world’s leading power in AI by 2030. Billions are being spent, and the Chinese have been unequivocal in their intent to develop AI for military use.

Absent U.S. and European investment in 5G wireless technology, China is successfully capturing next-generation cellular markets and equipment and infrastructure sales globally. The United States has been steadfast in its opposition to Chinese 5G expansion due to significant national security concerns. Granting Chinese companies access and control of the 5G spectrum allows the government of China to collect data and spy on its users, as well as control critical communications systems with the ability to interrupt or shut down networks in a conflict. A handful of countries—Australia, New Zealand, United Kingdom, Japan, and Vietnam—have joined the U.S. ban on Huawei; however, without a viable alternative, most countries remain undecided or have moved forward with Chinese technology.<sup>12</sup>

Since the 1970s, the United States has increasingly exported its manufacturing sector overseas—much of it to China. The practice has created supply chain risks and single points of failure vulnerabilities in everything from ammunition and surgical masks to components in fighter jets and cell phones. China’s control of U.S. pharmaceutical manufacturing, laid bare by the COVID-19 pandemic, has given it immense power over the health of the U.S. population.

Still, while China and the United States appear destined to be rivals, they maintain a complex yet symbiotic partnership that would be challenging for either country to upend, at least in the short term. Since restoring diplomatic relations with Beijing in 1979, the United States has deepened its social and economic ties with China, leading to increased prosperity in both countries. Recognizing these shared interests may allow for diplomatic endeavors and financial leverage to drive outcomes and to avoid seemingly inevitable conflict.

## **Russia**

Bellicose behavior by Russia to include military intervention in Ukraine, the annexation of Crimea, and meddling in U.S. and European elections has led to an increasingly adversarial relationship with the United States, and the potential for near-term conflict is rising swiftly. Large energy reserves drive Russia’s economy and allow the country to utilize this significant revenue source to their economic and military advantage.

Russian President Vladimir Putin’s aspirations to reestablish an era of Soviet power and prestige have led to aggressive actions and a return to authoritarianism. Similar to the political

<sup>11</sup> New York Times, *China Want AI to Be Made in China by 2050* (Jul. 20, 2017) (online at <https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html>).

<sup>12</sup> David E. Sanger and David McCabe, *Huawei Is Winning the Argument in Europe, as the U.S. Fumbles to Develop Alternatives*, New York Times (Feb. 17, 2020) (online at <https://www.nytimes.com/2020/02/17/us/politics/us-huawei-5g.html>).

machinations that President Xi used to secure his lifetime grip on power in China,<sup>13</sup> Putin is maneuvering to end term limits to the Russian presidency, essentially allowing him to serve for life.<sup>14</sup>

Russia is increasing its ability to challenge the United States and its security partners across multiple warfare platforms to include conventional and strategic weapons while also increasing its military and political presence in key locations globally.<sup>15</sup> It is also increasing its military spending in the Arctic to strengthen its territorial defense capabilities while further seeking to control the Northern Sea Route (NSR). In 2014, Russia formed the Northern Fleet Joint Strategic Command and ramped up military basing and infrastructure along the Arctic coastline.<sup>16</sup>

Fueled by arctic warming that is rapidly shrinking the northern ice cap, the NSR has become an epicenter of growing competition. Its potential as a shipping route between Europe and Asia could change global trade flows, and the massive hydrocarbon reserves that lie beneath it could significantly alter energy markets. One-tenth of Russia's economic investments are currently in the Arctic region.<sup>17</sup> Since 2013, Russia has spent billions of dollars building or upgrading military bases on islands and peninsulas along the NSR, deploying advanced radar and missile defense systems and giving Russia nearly complete coverage of the entire coastline and adjacent waters.<sup>18</sup>

China and Russia, who are more aligned now than at any other time since the 1950s,<sup>19</sup> are reported to have agreed jointly to build an "Ice Silk Road" on the NSR along a maritime route that Russia considers to be part of its internal waters. Chinese and Russian companies are seeking cooperation on oil and gas exploration in the area as well as collaborating on infrastructure construction, tourism, and scientific expeditions.

As Russia looks to avoid military escalation with the United States and its allies, it is increasing its ability to operate in the gray zone by using tactics such as propaganda and disinformation campaigns, political influence,<sup>20</sup> economic coercion, and proxy forces.<sup>21</sup>

In the Middle East, Africa, and South America, Russia is leveraging private military corporations (PMCs) such as the Wagner Group and others to conduct military operations and

<sup>13</sup> BBC News, *Xi Allowed to Remain President for Life as Term Limits Removed* (Mar. 11, 2018) (online at <https://www.bbc.com/news/world-asia-china-43361276>).

<sup>14</sup> The Associate Press, *Putin Approves Law That Could Keep Him in Power Until 2036* (Mar. 14, 2020) (online at <https://apnews.com/0885663075a29fbf5cc1d3c44894f4b9>).

<sup>15</sup> Government Accountability Office, *Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies* (Dec. 2018) (online at <https://www.gao.gov/assets/700/695981.pdf>).

<sup>16</sup> Department of Defense, *Report to Congress Arctic Strategy* (Jun. 2019) (online at <https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF>).

<sup>17</sup> Financial Times, *Polar Powers: Russia's Bid for Supremacy in the Arctic Ocean* (Apr. 27, 2019) (online at <https://www.ft.com/content/2fa82760-5c4a-11e9-939a-341f5ada9d40>).

<sup>18</sup> Department of Defense, *Report to Congress Arctic Strategy* (Jun. 2019) (online at <https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF>).

<sup>19</sup> Officer of the Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Jan. 29, 2019) (online at <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>).

<sup>20</sup> Michael Schwartz and Gaelle Borgia, *How Russia Meddles Abroad for Profit: Cash Trolls and Cult Leader*, New York Times (Nov. 11, 2019) (online at <https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html>).

<sup>21</sup> Kathleen H. Hicks, *Russia in the Gray Zone*, Center for Strategic and International Studies (Jul. 25, 2019) (online at <https://www.csis.org/analysis/russia-gray-zone>).

campaigns. The private nature of the force, which often comprises former members of Russian military and intelligence forces, allows Russia plausible deniability and accountability for military actions.<sup>22</sup> Russia has used PMCs for both military influence and political gain in Ukraine, Venezuela, Syria,<sup>23</sup> Libya, and the Central African Republic, among other countries.

For decades, Russia has meddled in elections; however, since 2014, it has stepped up its interference in Western democracies to include France, Germany, Norway, the United Kingdom, and the United States.<sup>24</sup>

Russia has also invested significantly in its cyberattack capacity and developed large-scale espionage capabilities. It has designed an ecosystem to ensure resilience and to attack in waves against election systems, power grids, transportation networks, and financial services.<sup>25</sup>

## North Korea

Under the leadership of Kim Jong-un, North Korea continues its unabated march toward full nuclearization. In July 2017, North Korea successfully launched its first intercontinental ballistic missile, which is likely capable of striking the United States.<sup>26</sup> Since then, it has continued to build and test increasingly sophisticated nuclear weapons and missiles, even as it suffers heavy sanctions by the international community.

Of further concern, especially to U.S. security partners South Korea and Japan, is North Korea's significant production and stockpile of biological and chemical weapons.<sup>27</sup> North Korea also maintains an exceptionally large conventional military force, a significant threat to regional allies and U.S. forces in the Pacific.<sup>28</sup>

## Iran

Long-simmering tensions between the United States and Iran reached a boiling point following the breakdown of the Joint Comprehensive Plan of Action (JCPOA). The return of sanctions against Iran and the U.S. military operation that resulted in the death of Qasem Soleimani,

<sup>22</sup> Andrew Linder, *Russian Private Military Companies in Syria and Beyond*, Center for Strategic and International Studies (Oct. 17, 2018) (online at <https://www.csis.org/npfp/russian-private-military-companies-syria-and-beyond>).

<sup>23</sup> Thomas Gibbons-Neff, *How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria*, New York Times (May 24, 2018) (online at <https://www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html>).

<sup>24</sup> Lucan Ahmad Way and Adam Casey, *Russia Has Been Meddling in Foreign Elections for Decades. Has it Made a Difference?*, The Washington Post (Jan. 8, 2018) (online at <https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/05/russia-has-been-meddling-in-foreign-elections-for-decades-has-it-made-a-difference/>).

<sup>25</sup> Italy Cohen and Omri Ben Bassat, *Checkpoint Report, Mapping the Connections Inside Russia's APT Ecosystem*, (Sept. 24, 2019) (online at <https://research.checkpoint.com/2019/russianaptecossystem/>).

<sup>26</sup> Choe Sang-Hun, *U.S. Confirms North Korea Fired Intercontinental Ballistic Missile*, The New York Times (Jul. 4, 2017) (online at <https://www.nytimes.com/2017/07/04/world/asia/north-korea-missile-test-icbm.html>).

<sup>27</sup> Nuclear Threat Initiative, *North Korea* (Aug. 2019) (online at <https://www.nti.org/learn/countries/north-korea/>).

<sup>28</sup> Eleonor Albert, *North Korea's Military Capabilities*, Council on Foreign Relations, Eleonor Abbot (Dec. 20, 2019) (online at <https://www.cfr.org/backgrounder/north-koreas-military-capabilities>).

leader of the Quds Force and the Islamic Revolutionary Guard Corps, severely diminished any chance of cooperation between Iran and the United States in the near term.

In the wake of the U.S. withdrawal from the JCPOA, Iran is increasing its uranium enrichment,<sup>29</sup> the first of many technological steps necessary to becoming a nuclear state.<sup>30</sup> While the United States is out, the other signatories, China, Russia, the United Kingdom, France, Germany, and the European Union, continue to adhere to the tenets of the agreement.

Iran has stepped up its attacks on oil production and shipping in the Persian Gulf and has brazenly attacked U.S. forces in Iraq.<sup>31</sup> It has deftly used proxy forces for decades, most recently in Yemen and Syria.<sup>32</sup> These actions against the United States and its Middle Eastern partners continue to push fragile boundaries, which may easily draw the United States into conflict with Iran or its proxies.<sup>33</sup>

Along with Russia and China, Iran has developed significant cyber warfare capabilities and has used them to attack U.S. banks and businesses as well as government entities.<sup>34</sup>

## **The Weaponization of Emerging Technologies**

Rapidly advancing technologies, which offer tremendous opportunity for civil and commercial applications, are also rife with potential for nefarious use and will exacerbate threat streams exponentially for the United States and its global partners. A sophisticated array of new weaponry is changing the nature of conflict, and, while most of the technologies will require substantial funding and development by state actors, others, such as cyber and electronic warfare, may allow less formidable foes to gain the operational upper hand with limited investment, with potentially limited ability to trace the source of such actions and hold those nations accountable.

Dual-use and lethal emerging technologies:

- AI – Potential military applications include intelligence collection and analysis, logistics, cyber operations, information operations, command and control, and autonomous vehicles.<sup>35</sup>

<sup>29</sup> NPR, *Iran Takes Another Step to Enrich Uranium in a Blow to Nuclear Deal* (Nov. 5, 2019) (online at <https://www.npr.org/2019/11/05/776387549/iran-takes-another-step-to-enrich-uranium-in-another-blow-to-nuclear-deal>).

<sup>30</sup> Nuclear Threat Initiative, *Iran* (Jan. 2020) (online at <https://www.nti.org/learn/countries/iran/nuclear/>).

<sup>31</sup> BBC News, *UK Soldier and Two Americans Killed in Rocket Attack in Iraq* (Mar. 12, 2020) (online at <https://www.bbc.com/news/world-middle-east-51842744>).

<sup>32</sup> Claire Parker and Rick Noack, *Iran has Invested in Allies and Proxies Across the Middle East, Here's Where They Stand After Soleimani's Death*, Washington Post (Jan. 3, 2020) (online at <https://www.washingtonpost.com/world/2020/01/03/iran-has-invested-allies-proxies-across-middle-east-heres-where-they-stand-after-soleimanis-death/>).

<sup>33</sup> David D. Kirkpatrick and Ben Hubbard, *Attack on Saudi Oil Facilities Tests U.S. Guarantee to Defend Gulf*, New York Times (Sept. 19, 2019) (online at <https://www.nytimes.com/2019/09/19/world/middleeast/saudi-iran-attack-oil.html>).

<sup>34</sup> Shannon Bond, *Iran Conflict Could Shift to Cyberspace, Experts Warn*, NPR (Jan. 21, 2020) (online at <https://www.npr.org/2020/01/21/797449708/iran-conflict-could-shift-to-cyberspace-experts-warn>).

<sup>35</sup> Daniel S. Hoadley and Kelley M. Sayler, *Artificial Intelligence and National Security*, Congressional Research Service (Aug. 26, 2020) (online at <https://fas.org/sgp/crs/natsec/R45178.pdf>).



- Biotechnology – Neuroscience, gene editing, and the proliferation of synthetic biology may lead to an increase in chemical and biological weapons.
- Lethal Autonomous Weapons – A weapons system capable of independently engaging and destroying a target without human control.
- Cyber Warfare – Adversaries may use cyber capabilities for military advantage, espionage, and critical infrastructure attacks, or seek political or economic influence.
- Electronic Warfare – Electronic attack capabilities could target sensitive electronic components to degrade military and civilian operations and infrastructure.
- Space and Counterspace – Along with the expansion of commercial space services and satellites, there is significant potential for the militarization of space.
- Hypersonic Weapons – Increased speed, altitude, and maneuverability may defeat U.S. missile defense systems while improving long-range conventional and nuclear strike capabilities for adversaries.
- Directed Energy – Weapons systems that use concentrated electromagnetic energy rather than kinetic energy. Often referred to as lasers, directed energy weapons also include high-powered microwave (HPM).
- Quantum Information Science – Quantum computing could enable adversaries to develop secure communications that the United States would not be able to intercept or decrypt. It may also allow adversaries to decrypt sensitive U.S. information.

## **A Divisive Homeland**

As internal strife festers and the United States focuses inward, American adversaries have been working overtime to secure global influence and power, both politically and militarily. And a divided America is playing distinctively into the hands of U.S. rivals.<sup>36</sup> Deepening ideological fissures in the United States have become incubators for disinformation campaigns and subversion by the Russian and Chinese governments, who have mastered the ability to weaponize a free and open society. The advent of social media has provided adversaries the perfect non-lethal weapon to inflict harm by sowing discord among Americans. Foreign intelligence services directly stream divisive content into personal media platforms, where a receptive public disseminates it.<sup>37</sup>

<sup>36</sup> Kevin R. Brock, *Coronavirus Wake-up Call: A Bigger National Security Threat Is at Work*, The Hill (Mar. 18, 2020) (online at <https://thehill.com/opinion/national-security/488182-coronavirus-wake-up-call-a-bigger-national-security-threat-is-at>).

<sup>37</sup> *Id.*

Failure to recognize and thwart these gray zone tactics is severely undermining the strength of the American republic, and there is increasing agreement among national security experts that rising polarization may be among the greatest threats to U.S. national security.<sup>38</sup>

## **Terrorism and Transnational Criminal Organizations**

Non-state actors specializing in malign activities threaten both the homeland as well as vital U.S. interests and partners abroad. VEOs and TNOs operating in the gray zone will continue to wreak havoc on local populations, destabilize governments, and drive migration.

As the United States draws down in Afghanistan, the country remains vulnerable to VEOs and TNOs as well as nefarious Russian and Iranian influence, among others.<sup>39</sup> History may repeat itself as a modern version of the 19<sup>th</sup> century Great Game plays out once again in Central Asia.<sup>40</sup>

Al Qaeda, ISIS, Al Shabab, and other terrorist organizations continue to operate in the Middle East, Africa, and Asia and threaten vital U.S. national security interests. Though Al Qaeda was weakened after the death of its founder, Osama bin Laden, it has evolved and reconstituted itself and now operates in more countries with more fighters than when it attacked the United States on 9/11.<sup>41</sup> And while ISIS has been denied the territory it initially secured in Iraq and Syria when it declared itself a caliphate, the premature U.S. pullout of Syria leaves it significant room to reorganize and build.<sup>42</sup> ISIS is further mounting resurgent campaigns in Afghanistan, Yemen, and multiple points in Africa.<sup>43</sup>

In the Western Hemisphere, TNOs operating in illicit trade such as drug and human trafficking are responsible for skyrocketing murder rates and untold human suffering.<sup>44</sup> VEOs and TNOs, which often work together, also threaten economies and markets globally through subversion and exploitation.<sup>45</sup>

<sup>38</sup> Dina Smeltz, Joshua Busby, and Jordan Tama, *Political Polarization the Critical Threat to US, Foreign Policy Experts Say*, The Hill (Nov. 9, 2018) (online at <https://thehill.com/opinion/national-security/415881-political-polarization-is-the-critical-threat-to-us-foreign-policy>).

<sup>39</sup> Lara Seligman, *As U.S. Mulls Withdrawal from Afghanistan, Russia Wants Back In*, Foreign Policy (Jan. 31, 2019) (online at <https://foreignpolicy.com/2019/01/31/us-mulls-withdrawal-from-afghanistan-russia-wants-back-in-taliban-peace-talks/>).

<sup>40</sup> Mark Gilchrist, *The Great Game Reinvigorated: Geopolitics, Afghanistan, and the Importance of Pakistan*, Real Clear Defense (Apr. 15, 2019) (online at [https://www.realcleardefense.com/articles/2019/08/15/the\\_great\\_game\\_reinvigorated\\_geopolitics\\_afghanistan\\_and\\_the\\_importance\\_of\\_pakistan\\_114667.html](https://www.realcleardefense.com/articles/2019/08/15/the_great_game_reinvigorated_geopolitics_afghanistan_and_the_importance_of_pakistan_114667.html)).

<sup>41</sup> Bruce Hoffman and Jacob Ware, *Al-Qaeda: Threat or Anachronism?*, War on the Rocks (Mar. 12, 2020) (online at <https://warontherocks.com/2020/03/al-qaeda-threat-or-anachronism/>).

<sup>42</sup> Colin P. Clarke, *How the U.S. Withdrawal from Syria Provides a Boost to ISIS*, RAND Corporation (Oct. 21, 2019) (online at <https://www.rand.org/blog/2019/10/how-the-us-withdrawal-from-syria-provides-a-boost-to.html>).

<sup>43</sup> Joseph Hincks, *With the World Busy With COVID-19, Could ISIS Mount an Insurgence?*, Time (Apr. 29, 2020) (online at <https://time.com/5828630/isis-coronavirus/>).

<sup>44</sup> Amelia Cheatham, *Central America's Turbulent Northern Triangle*, Council on Foreign Relations (Oct. 1, 2019) (online at <https://www.cfr.org/background/central-americas-turbulent-northern-triangle>).

<sup>45</sup> National Security Council, *Transnational Organized Crime: A Growing Threat to National and International Security* (online at <https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat>).

## Climate Change Is a Threat Multiplier

In a 2019 report to congress, the DOD issued a high-level assessment of current and future national security vulnerabilities due to climate change and outlined climate change's impact on DOD missions, operational plans, and infrastructure as a result of drought, flooding, desertification, wildfires, and a thawing permafrost.<sup>46</sup> Climate change has been determined by the defense and intelligence communities to be a threat multiplier because it significantly intensifies and accelerates existing threat streams.<sup>47</sup> The resiliency of current military installations and decisions regarding future military basing must take into account rising sea levels, climate change, and the availability of resources.

Increasingly volatile and extreme weather patterns and pollution will lead to environmental degradation resulting in rising sea levels, ocean acidification, glacial melt, and soil erosion. Second- and third-order effects could include increased competition for resources, water and food insecurity, famine, infectious diseases and pandemics, migration and human displacement, and increased potential for open conflict.<sup>48</sup>

Changing weather patterns may also affect food security. The United States is a global superpower, in part because it can feed both itself and much of the rest of the world. Immense farmlands, fresh water, and extensive growing seasons allow the United States a wealth of food security. Advancements in biotechnology will eventually change this equation and level the playing field, but for the foreseeable future, the United States should recognize this powerful capability and work to protect it from threats such as climate change, the decline of family-owned farms and ranches,<sup>49</sup> and foreign investment in U.S. agricultural holdings.

For more than two decades, foreign entities have been buying up U.S. farmland,<sup>50</sup> and now, some 30 million acres of agricultural land, larger than the state of Tennessee, is foreign-owned. Over the last decade, Chinese investment in U.S. agriculture has surged exponentially to include the acquisition of Virginia-based Smithfield Foods, the largest pork producer in the world.<sup>51</sup> There is increasing bipartisan and bi-cameral legislative support to limit the sale of both agricultural holdings to foreign entities and the sale of critical infrastructure deemed necessary to national security.

<sup>46</sup> Department of Defense, *Report on the Effects of Climate Change* (Jan. 10, 2019) (online at <https://media.defense.gov/2019/Jan/29/2002084200/-1/-1/1/CLIMATE-CHANGE-REPORT-2019.PDF>).

<sup>47</sup> Mark Nevitt, *Climate Change: Our Greatest National Security Threat?*, Just Security (Apr. 17, 2019) (online at <https://www.justsecurity.org/63673/climate-change-our-greatest-national-security-threat/>).

<sup>48</sup> Office of the Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (Jan. 29, 2019) (online at <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>).

<sup>49</sup> Helianti Hillman, *Why Family Farmers Are the Key to Global Food Security*, World Economic Forum (Apr. 17, 2015) (online at <https://www.weforum.org/agenda/2015/04/why-family-farmers-are-the-key-to-global-food-security/>) and Department of Agriculture, National Institute of Food and Agriculture (online at <https://nifa.usda.gov/topic/small-and-family-farms>).

<sup>50</sup> Renee Wild, *'American Soil' Is Increasingly Foreign Owned*, NPR (May 27, 2019) (online at <https://www.npr.org/2019/05/27/723501793/american-soil-is-increasingly-foreign-owned>).

<sup>51</sup> Jennifer Wang, *The Chinese Billionaire Whose Company Owns Troubled Pork Producer Smithfield Foods*, Forbes (Apr. 16, 2020) (online at <https://www.forbes.com/sites/jenniferwang/2020/04/16/the-chinese-billionaire-whose-company-owns-troubled-pork-processor-smithfield-foods/#1996f8f72c55>).



## EMERGING TECHNOLOGIES

A sophisticated array of emerging technologies and new weaponry, in various stages of development, will fundamentally change the nature of conflict along with the very battlespace where it will be fought. The stakes are high. Whoever achieves superiority in this technological race will enjoy significant military and economic advantages for decades, and possibly into the next century. Achieving this supremacy will require a whole of nation approach where the distinct advantages of both the private and public sectors are harnessed and synthesized.

While these technologies offer tremendous opportunity for commercial and social transformation, they are also rife with the potential for nefarious use and may exacerbate threat streams exponentially for the United States and its global partners.

Advancements in artificial intelligence (AI), quantum information science, and cyber and electronic warfare, among other fields, are making traditional battlefields and boundaries increasingly irrelevant. To remain competitive, the United States must recognize this shift and prioritize the development of emerging technologies while also increasing its ability to defend against them.

### **The David Versus Goliath Paradigm**

As adversaries build and recapitalize conventional and strategic weapons, there is a parallel effort to develop systems that adhere to the David and Goliath paradigm: Instead of taking on the giant pound for pound, build nimble and inexpensive sling shots.

Technology is pulling warfare into a post-conventional era where the first hours of conflict will no longer be saturated with aerial bombings and sea landings followed by a ground assault. Initial campaigns will be fought with remote and autonomous systems in the realms of space and cyberspace, where an early attack will take out satellite and communication systems and dismantle the Global Positioning System (GPS). Opening salvos could inflict devastating harm on civilians through electronic attacks on critical infrastructure and power grids, along with financial and healthcare systems and networks.

Competitors may deploy these covert and gray-zone tactics to avoid a traditional U.S. military response. And because vast swaths of emerging technologies are being developed in the private sector, both state and non-state actors will have access to them, which may prove vexing to defend against. Not knowing or understanding who the enemy is, or where the attack is coming from, will exacerbate threat streams and limit counterstrike capability.

### **Artificial Intelligence**

AI will impact nearly every aspect of society and has the potential to be one of the key economic drivers over the next century.<sup>52</sup> The incorporation of AI into the military and national

<sup>52</sup> Department of Commerce, *Why is Artificial Intelligence Important?*, National Institute of Standards and Technology (online at <https://www.nist.gov/topics/artificial-intelligence>).

security realms will fundamentally change the way wars are fought and won. Whichever nation triumphs in the AI race will hold a critical, and perhaps insurmountable, military and economic advantage.

AI allows a computer to think, learn, and perform in the cognitive ways that humans operate. Soon, advanced AI ecosystems will see machines surpassing human capability in speed, analyzation of large data sets, and pattern recognition.<sup>53</sup> Advancement in AI will shape the global power structure and drive advancements in commerce, transportation, health, education, financial markets, government, and national defense.<sup>54</sup>

The weaponization of AI will bring complex security challenges, among them the concept that an activated autonomous AI system will engage targets without human guidance or intervention. The advent of algorithmic warfare,<sup>55</sup> where AI-enabled weaponry driven by speed and precision compete in a complex battlespace, requires the United States to invest significantly in both offensive and defensive AI capabilities.

Because the rise of AI carries the unique ability to attack democracy through the suppression of personal freedoms and civil liberties, it is unique among emerging technological threats. The integration of AI into surveillance through facial recognition and other monitoring capabilities makes AI rife with potential for human rights abuse and repression. Currently, more than a third of all countries, including many western-style democracies, already employ some form of AI surveillance.<sup>56</sup>

While multiple developed countries are investing in AI, China is a primary exporter of surveillance technology.<sup>57</sup> In 2017, China announced, along with its plan to become a global superpower by 2050, its “New Generation Artificial Intelligence Development Plan” and set the ambitious goal of becoming the world’s leading power in AI by 2030. There is increasing concern that the export of these Chinese-developed technologies and the globalization of the Chinese surveillance state could also result in widespread data collection and human rights abuses.

In its highly robust 2019 interim report, the National Security Commission on Artificial Intelligence was unequivocal in its analysis of how AI will be a game-changer. “AI will shape the future of power. The nation with the most resilient and productive economic base will be best positioned to seize the mantle of world leadership. That base increasingly depends on the strength of the innovation economy, which in turn will depend on AI. AI will drive waves of advancement in commerce, transportation, health, education, financial markets, government, and national defense.”<sup>58</sup>

<sup>53</sup> National Security Commission on Artificial Intelligence, *Interim Report* (Nov. 2019) (online at <https://drive.google.com/file/d/153OrxnuGEjsUvIxWsFYauslwNeCEkvUb/view>).

<sup>54</sup> *Id.*

<sup>55</sup> *Id.*

<sup>56</sup> The Carnegie Endowment for International Peace, *The Global Expansion of AI* (Sept. 2019) (online at <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>).

<sup>57</sup> *Id.*

<sup>58</sup> National Security Commission on Artificial Intelligence, *Interim Report* (Nov. 2019) (online at <https://drive.google.com/file/d/153OrxnuGEjsUvIxWsFYauslwNeCEkvUb/view>).

To integrate and accelerate the adoption of AI, the Department of Defense (DOD) has created the Joint Artificial Intelligence Center (JAIC), which, along with its mandate to synchronize and scale AI within the DOD, partners with academia and industry to develop AI strategy, planning, and implementation.<sup>59</sup> Potential military applications include intelligence collection and analysis, logistics, cyber operations, information operations, command and control, and autonomous vehicles, among others.<sup>60</sup>

## Biotechnology and Bio Threats

Biotechnology is the field of applied science that harnesses and manipulates cellular and biomolecular processes to create products and develop technology. As one of many emerging dual-use technologies, advancements in biotech will significantly alter both the health and food sciences, and the potential for civilian applications is nearly immeasurable.

Advancements in biotechnology are creating new domains of warfare that are being aggressively pursued by potential adversaries, including China. Elsa Kania, who appeared before the Task Force and has extensively researched the Chinese People's Liberation Army (PLA), writes that the PLA is pursuing military biotech dominance as well as the intersection of AI and biotech.<sup>61</sup>

The proliferation of biotechnology for military applications could see the altering of genetic code to modify plants, animals, and humans, and could be used to enhance the performance of military personnel.<sup>62</sup> Advancements in synthetic biology, which creates genetic code that does not exist in nature, may increase the development of chemical and biological weapons.<sup>63</sup> An extreme application would be a biological form of warfare that targets a specific ethnic group. Biotech is already being used to alter food, seeds, and animals, and it could also be used to strengthen some economies and nations while weakening or causing unrest in others.

Weaponized biotechnology remains a unique threat to the homeland, where attacks on food and water supplies would indiscriminately harm civilians. The COVID-19 pandemic lays bare the vast array of vulnerabilities the United States must overcome to predict, thwart, and recover from a biological attack. It further exposes the weaknesses in the food supply chain that could be easily exploited by the nefarious use of biotechnology.

<sup>59</sup> Summary of Department of Defense AI Strategy, *Harnessing AI to Advance Our Security and Prosperity* (2018) (online at <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF>).

<sup>60</sup> Congressional Research Service, *Artificial Intelligence and National Security* (Aug. 26, 2020) (online at <https://fas.org/sgp/crs/natsec/R45178.pdf>).

<sup>61</sup> Elsa Kania and Wilson Vorndick, *Weaponizing Biotech: How China is Preparing for a New Domain of Warfare*, Defense One (Aug. 14, 2019) (online at <https://www.defenseone.com/ideas/2019/08/chinas-military-pursuing-biotech/159167/>).

<sup>62</sup> Government Accountability Office, *Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies* (Dec. 2018) (online at <https://www.gao.gov/assets/700/695981.pdf>).

<sup>63</sup> *Id.*

## Lethal Autonomous Weapons

Lethal autonomous weapons will reimagine future conflicts and present significant operational, legal, and ethical challenges. They could lessen casualties by more accurately differentiating combatants from civilians, or conversely, they could be deployed indiscriminately on a new and horrific scale.

One activated, lethal autonomous weapons system (LAWS) will select and engage targets without further human intervention.<sup>64</sup> The development of robotics and AI will increase the precision and lethality of autonomous weapons, especially in the case of swarm tactics, where large numbers attack and overwhelm a target.

The development of LAWS remains in the nascent stage; however, given the certainty that adversarial nations are developing autonomous weapons, the United States is investing broadly in advanced military applications of autonomous systems.<sup>65</sup> Equally important will be the need to develop strong defensive capabilities against LAWS.

It is imperative that policy experts and lawmakers consider the second- and third-order effects of developing and deploying LAWS. Moral, ethical, and legal factors will need to be weighed accordingly. Approximately 25 countries have already called for banning autonomous weapons.<sup>66</sup> Currently, the United States does not support a ban, arguing that the use of LAWS will increase targeting accuracy and reduce civilian casualties.<sup>67</sup> In addition, Pentagon guidance requires that “appropriate levels of human judgment” preside over the use of force by LAWS, although what is appropriate is open to broad interpretation.

## Cyber Warfare

Cyber warfare and cyberattack capability will proliferate and expand the scope of conflict beyond traditional borders or battle lines as the use of computers, networking, and automation becomes pervasive in nearly every aspect of modern life. Because of this ubiquity, private, public, and defense entities are all targets for cyberattack, making the homeland and civilian population uniquely vulnerable. And dominance or control of the 5G spectrum could more readily enable cyberattacks by adversaries.

Adversaries may use cyberattack capabilities for political or economic influence, military advantage, espionage, or critical infrastructure attacks on financial networks, healthcare facilities, or

<sup>64</sup> Department of Defense Directive 3000.09 (Nov. 21, 2012).

<sup>65</sup> Department of Defense, *National Defense Strategy* (2018) (online at <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>).

<sup>66</sup> Kelley M. Saylor, *Defense Primer: U.S. Policy on Lethal Autonomous Weapons*, Congressional Research Service (Dec. 2019) (online at <https://fas.org/sgp/crs/natsec/IF11150.pdf>).

<sup>67</sup> Department of State, *U.S. Statement on LAWS, Potential Military Applications of Advanced Technology*, U.S. Mission to International Organizations in Geneva (Mar. 25, 2019) (online at <https://geneva.usmission.gov/2019/03/26/u-s-statement-on-laws-potential-military-applications-of-advanced-technology/>).



public utilities. The ability of non-state actors to engage in cyber warfare gives significant capability to rogue or malign individuals or groups who would otherwise be less threatening.

As the United States increases its engagement in offensive cyber operations, it must also increase its ability to defend against deliberate and sustained cyberattacks on both civilian and military targets. This is especially critical due to the computerization and networking of weapons systems, making them vulnerable to a cyberattack.<sup>68</sup>

## Electronic Warfare

Warcraft in the future will increasingly rely on electronic sabotage, where adversaries seek to disrupt and disable systems and networks before any fighting begins.

Electronic attack weapons target systems with sensitive electronic components, such as military sensors, communication, navigation, and information systems. They are intended to degrade capabilities and restrict communications to affect military operations.<sup>69</sup> Bereft of strong countermeasures, electronics remain a vulnerable platform to the David and Goliath paradigm, where a smaller, less capable adversary gains the initial upper hand through disruption.

The weaponization of the electromagnetic spectrum through the use of electromagnetic pulse (EMP) and other attack measures is underway and increasingly being used in gray zone tactics.<sup>70</sup> As an example, because of its vulnerability to electronic attack, the Defense Advanced Research Project Agency (DARPA) now considers GPS to be a single point of failure in the U.S. military apparatus.<sup>71</sup>

## Space and Counterspace Weapons

Whichever nation maintains control of space and retains the ability to use it to communicate, navigate, and see anywhere in the world almost instantaneously—in both peace and wartime—will enjoy a decisive advantage.

The democratization of space in the 21<sup>st</sup> century has opened new frontiers in both the commercialization and militarization of space. The technological ecosystems created by these advancements requires the United States to build out its offensive and defensive capabilities.

Alongside strategic weapons are a spate of emerging technologies that are increasingly being deployed in space to include electronic warfare, directed energy and kinetic energy attacks, and cyber

<sup>68</sup> Government Accountability Office, *Weapons Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities* (Oct. 9, 2018) (online at <https://www.gao.gov/products/GAO-19-128>).

<sup>69</sup> Government Accountability Office, *Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies* (Dec. 2018) (online at <https://www.gao.gov/assets/700/695981.pdf>).

<sup>70</sup> Jayshree Pandya, *The Weaponization of the Electromagnetic Spectrum*, *Forbes* (Apr. 12, 2019) (online at <https://www.forbes.com/sites/cognitiveworld/2019/04/12/the-weaponization-of-the-electromagnetic-spectrum/#2a8c3c8f699e>).

<sup>71</sup> Sarah Scoles, *Spoof, Jam, Destroy: Why We Need a Backup for GPS*, *Wired* (Mar. 2, 2018) (online at <https://www.wired.com/story/spoof-jam-destroy-why-we-need-a-backup-for-gps/amp>).

threat.<sup>72</sup> Offensive capabilities include anti-satellite missiles, EMP, laser and microwave, jamming and spoofing, and data interception and control.<sup>73</sup>

The reliance on space-based technology for both civilian and military applications requires that U.S. defensive capabilities be strengthened and fortified. Communication satellites; intelligence, surveillance, and reconnaissance (ISR); positioning, navigation, and targeting (PNT); and other technologies remain vulnerable to attack by both state and non-state actors.<sup>74</sup>

China and Russia are increasing their ability to challenge the United States in space and reorganized their militaries in 2015 to emphasize the importance of space and counter-space operations.<sup>75</sup> Both are developing jamming and cyberspace capabilities, directed energy weapons, and ground-based antisatellite missiles.<sup>76</sup> Iran and North Korea are also developing significant counterspace capabilities.<sup>77</sup>

## Hypersonic Weapons

Hypersonic weapons will increase the speed and distance of modern conflict. Hypersonic glide vehicles and hypersonic cruise missiles are maneuverable, long-range weapons that fly at a speed of Mach 5 or greater and do not follow a ballistic trajectory but rather can maneuver while traveling to their target.<sup>78</sup> Their ability to change course after being launched from either a conventional or strategic weapon may allow them to defeat missile defense systems and strike targets from significant stand-off distances.<sup>79</sup>

Hypersonic weapons will create complex battle management scenarios due to the speed and range at which they can strike. The extreme tempo may also significantly degrade the ability to deploy countermeasures.<sup>80</sup> The use of hypersonic weapons for Prompt Global Strike (PGS) capability, where conventional weapons take out high-value or fleeting strategic targets early in a conflict, has garnered increased support in Congress and the Pentagon.<sup>81</sup> While intended to be a deterrent or to limit adversarial ability to use anti-access, area denial (A2/AD) capability, it is also

<sup>72</sup> Center for Strategic and International Studies, *Counterspace Weapons 101*, Aerospace Security (Jul. 23, 2020) (online at <https://aerospace.csis.org/aerospace101/counterspace-weapons-101/>).

<sup>73</sup> *Id.*

<sup>74</sup> Defense Intelligence Agency, *Challenges to Security in Space* (Jan. 2019) (online at [https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space\\_Threat\\_V14\\_020119\\_sm.pdf](https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf)).

<sup>75</sup> *Id.*

<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

<sup>78</sup> Kelley M. Saylor, *Hypersonic Weapons: Background and Issues for Congress*, Congressional Research Service (Aug. 27, 2020) (online at <https://fas.org/sgp/crs/weapons/R45811.pdf>).

<sup>79</sup> Kelley M. Saylor and Amy F. Woolf, *Defense Primer: Hypersonic Boost-Glide Weapons*, Congressional Research Service (Mar. 13, 2020) (online at <https://crsreports.congress.gov/product/pdf/IF/IF11459>).

<sup>80</sup> Sebastien Roblin, *The Pentagon Plans to Deploy and Arsenal of Hypersonic Weapons in the 2020s*, Forbes (Apr. 30, 2020) (online at <https://www.forbes.com/sites/sebastienroblin/2020/04/30/the-pentagons-plans-to-deploy-an-arsenal-of-hypersonic-weapons-in-the-2020s/>).

<sup>81</sup> Amy F. Woolf, *Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues*, Congressional Research Service (Feb. 14, 2020) (online at <https://fas.org/sgp/crs/nuke/R41464.pdf>).

fraught with the potential for miscalculation since an adversary could easily mistake a hypersonic conventional weapon for a nuclear one, thus increasing the risk of a nuclear response.<sup>82</sup>

In December 2019, Russia deployed the first hypersonic weapon capable of evading a U.S. missile defense system,<sup>83</sup> and China is expected to have operational capability in hypersonic glide vehicles by the end of 2020.<sup>84</sup> While the Pentagon's FY2021 budget request for hypersonic research is \$3.2 billion, there is currently no program of record for hypersonic weapons.<sup>85</sup>

## Directed Energy

Fully developed, directed energy weapons could provide a near-unlimited, inexpensive, and instantaneous supply of precise firepower without having to reload, resupply, or even manufacture munitions. They may further offer the most effective means to defend massed attacks from weapons such as swarming drones or a barrage of guided missiles.

Direct energy weapons use concentrated electromagnetic energy rather than kinetic energy to strike targets. Two types of weapons currently in development are high-energy lasers (HELs) and high-powered microwave (HPM).<sup>86</sup> Laser weapons essentially heat a target until it melts, while microwave weapons disrupt the electronics of a target.<sup>87</sup>

Directed energy weapons can operate as both a sensor and a weapon, which allows for multiple attacks on a target before an adversary can respond.<sup>88</sup> As a weapons system, they offer both offensive and defensive capabilities and are being rapidly developed by the United States Air Force, Navy, and Army.<sup>89</sup>

## Quantum Information Science

While still in the nascent stages of development, whoever establishes quantum supremacy will maintain tremendous strategic capability over their adversaries.

<sup>82</sup> *Id.*

<sup>83</sup> Julian E. Barnes and David E. Sanger, *Russia Deploys Hypersonic Weapon, Potentially Renewing Arms Race*, New York Times (Dec. 27, 2019) (online at <https://www.nytimes.com/2019/12/27/us/politics/russia-hypersonic-weapon.html>).

<sup>84</sup> Kelley M. Sayler, *Hypersonic Weapons: Background and Issues for Congress*, Congressional Research Service (Aug. 27, 2020) (online at <https://fas.org/sgp/crs/weapons/R45811.pdf>).

<sup>85</sup> *Id.*

<sup>86</sup> J.R. Wilson, *Directed Energy Weapons Taking Big Steps Forward*, Military and Aerospace Electronics (Jul. 1, 2019) (online at <https://www.militaryaerospace.com/unmanned/article/14036378/directedenergy-weapons-taking-big-steps-forward>).

<sup>87</sup> Shaun Waterman, *Directed Energy Weapons Move Closer to Primetime*, Department of Defense Joint Intermediate Force Capabilities Office (Oct. 29, 2019) (online at <https://jnlwp.defense.gov/Press-Room/In-The-News/Article/2020551/directed-energy-weapons-move-closer-to-prime-time/>).

<sup>88</sup> Andrew Feickert, *U.S. Army Weapons-Related Directed Energy Programs: Background and Potential Issues for Congress*, Congressional Research Service (Feb. 12, 2018) (online at <https://fas.org/sgp/crs/weapons/R45098.pdf>).

<sup>89</sup> *Id.*

Quantum computing is the compression and subsequent acceleration of information, which allows computers to process seemingly infinite possibilities simultaneously. Quantum communications could enable the development of communications and data that cannot be intercepted or decrypted. Likewise, it could be used to decrypt otherwise secure information at previously unknown speeds.<sup>90</sup> This capability will offer tremendous advantages both militarily and in the private sector.

There is increasing concern among U.S. scientists that China is leading in the quantum information science race due to recent gains in the theory of quantum entanglement whereby subatomic particles can be seemingly linked over great distances, thus allowing for quantum encryption.<sup>91</sup>

## Strategic Concepts and Ethics

It is essential that the United States recognize that adversaries seek to use many of these emerging technologies to dominate early in a conflict by disrupting and degrading both civilian and military systems and networks. The disruption of command, control, communications, computers, and ISR (C4ISR) has become a bedrock operational concept of 21<sup>st</sup> century warfare.<sup>92</sup> The ability of the United States to leverage offensive and defensive capabilities in this realm is paramount to maintaining the global balance of power as well as strategic and conventional military superiority.

Discoveries in AI, biotechnology, and quantum computing are on course to upend nearly every aspect human life and will drastically change how conflicts and wars are waged. Therefore, it is essential that democratic nations, who adhere to human rights, lead in their development and applications.

Further, it will be incumbent upon the nations who use these technologies to set strong moral and ethical standards to protect the health and well-being of humankind. Advancements in AI, for example, will likely require a global compact in the vein of the Geneva Conventions, the Chemical Weapons Convention, and the Nuclear Non-Proliferation Treaty to establish guardrails and protect against a variety of factors, not the least of which is the infringement of personal liberty and freedoms.

<sup>90</sup> Government Accountability Office, *Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies* (Dec. 2018) (online at <https://www.gao.gov/assets/700/695981.pdf>).

<sup>91</sup> William J. Broad, *China Reports Progress in Ultra-Secure Satellite Transmission*, The New York Times (Jun. 15, 2020) (online at [https://www.nytimes.com/2020/06/15/science/quantum-satellites-china-spying.html?algo=identity&fallback=false&imp\\_id=367663978&action=click&module=Science%20%20Technology&pgtype=Homepage](https://www.nytimes.com/2020/06/15/science/quantum-satellites-china-spying.html?algo=identity&fallback=false&imp_id=367663978&action=click&module=Science%20%20Technology&pgtype=Homepage)).

<sup>92</sup> Michele Flournoy and Gabrielle Chefitz, *Sharpening the U.S. Military's Edge: Critical Steps for the Next Administration*, Center for a New American Security (Jul. 13, 2020) (online at [https://www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration?utm\\_medium=email&utm\\_campaign=Defense+Launch+of+Next+Defense+Strategy+Project+press+release&utm\\_content=Defense+Launch+of+Next+Defense+Strategy+Project+press+release+CID\\_c709fecb79ba4caf85b2cc0ae4632700&utm\\_source=Campaign+Monitor&utm\\_term=Sharpening+the+US+Militarys+Edge+Critical+Steps+for+the+Next+Administration](https://www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration?utm_medium=email&utm_campaign=Defense+Launch+of+Next+Defense+Strategy+Project+press+release&utm_content=Defense+Launch+of+Next+Defense+Strategy+Project+press+release+CID_c709fecb79ba4caf85b2cc0ae4632700&utm_source=Campaign+Monitor&utm_term=Sharpening+the+US+Militarys+Edge+Critical+Steps+for+the+Next+Administration)).

## PARTNERS AND SECURITY ALLIANCES

To secure vital nation security interests both at home and abroad, the United States should embrace the doctrine of collective security by strengthening existing alliances and working to build new ones. A whole of government approach that engages global partners through diplomacy, economics, humanitarian aid, security cooperation, and military to military relations is among the most notable actions the United States can take to ensure continued peace, financial stability, and strategic overmatch when gaming out the future of defense.

Among the most oft-repeated recommendations by military officers, Department of Defense and government civilians, academics, and key leaders during the six-month investigation by the Future of Defense Task Force was the observation that the United States needs to bolster its security cooperation and diplomatic relationships to protect national security interests against rising threat streams, most notably the rise of a new form of authoritarianism<sup>93</sup> that seeks to emulate capitalism while weaponizing personal information and asserting ever greater government control.

The 2019 National Defense Strategy (NDS) aptly stated, “A more lethal, resilient, and rapidly innovating Joint Force, combined with a robust constellation of allies and partners, will sustain American influence and ensure favorable balances of power that safeguard the free and open international order.”<sup>94</sup>

### Strengthening Global Partnerships

To endure as a global democratic power with economic and political influence and a resilient forward military footprint, the United States must strengthen its geopolitical alliances with its longstanding allies while fostering relationships with new partners.

Sustaining robust ties with Five-Eye intelligence partners Canada, United Kingdom, Australia, and New Zealand, as well as with NATO, is essential. Equally important are the United States’ relationships with Japan and South Korea. Key allies in the Middle East, notably Israel and Jordan, among others, will continue to be vital U.S. partners. The United States should also cultivate economic and diplomatic cooperation with non-traditional allies, notably in Asia and in Africa where, in 20 years, one-third of the world’s workers will live.<sup>95</sup> The United States should also reengage in the Western Hemisphere with both Latin American and Arctic partners.

In Asia, the United States should seek to strengthen relations with long-standing security partners such as Thailand, the Philippines, Taiwan, and Singapore, while growing relationships with Vietnam, Indonesia, and Malaysia, among others. The United States could further benefit from

<sup>93</sup> Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism*, Brookings Institution (Aug. 2019) (online at <https://www.brookings.edu/research/exporting-digital-authoritarianism/>).

<sup>94</sup> Department of Defense, *National Defense Strategy* (2018) (online at <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>).

<sup>95</sup> Gilles Pison, *By 2100, A Third of People on Earth Will Be African*, World Economic Forum (Oct. 12, 2017) (online at <https://www.weforum.org/agenda/2017/10/there-s-a-strong-chance-that-one-third-of-all-people-will-be-african-by-2100>).

economic alliances such as the Asia-Pacific Economic Cooperation (APEC) and the World Trade Organization (WTO), and by establishing higher standards for trade and investment that would allow U.S. businesses to compete fairly.<sup>96</sup>

Africa, the new frontier for manufacturing,<sup>97</sup> is enjoying steady growth in several countries where, after years of colonial upheaval and civil wars, a middle class is slowly emerging. Its landmass, the area of which exceeds that of China, Europe, and the United States combined,<sup>98</sup> should be cause for recognition alone. In 20 years, Africa will replace Asia as the continent with the most workers.<sup>99</sup> Moreover, Africa is ground zero in the fight for the expansion of democracy. Both Russia and China are putting enormous resources into the African continent, and both are seeking military influence through a variety of measures that include arms sales, security agreements, and training programs.<sup>100</sup> Simply put, the United States cannot cede development, influence, and security on the African continent, and expect the world order to continue unchanged.

The United States must also reengage in Latin America and the Caribbean, where China is making significant economic and political gains through the Belt and Road Initiative. Arguing that it is a natural extension of their 21<sup>st</sup> Century Maritime Silk Road,<sup>101</sup> China has ongoing development projects in 19 of the 33 Latin American countries. By willfully pursuing such weighty economic, diplomatic, and military endeavors in the Western Hemisphere, China is putting to rest any notion that it only seeks to be a regional hegemon. In a return to Cold War machinations, Russia is increasingly meddling in South America in what appears to be an attempt to stifle democratic influence through disinformation campaigns and the deployment of proxy fighters.<sup>102</sup>

The thawing of the Arctic is creating seismic economic and political shifts as the region emerges as an epicenter of the 21<sup>st</sup> century Great Game. Russia, a natural competitor in the region due to its nearly 15,000 miles of Arctic coastline,<sup>103</sup> is the most aggressive, having committed significant financial and military resources to the region. Its provocative expansion of former Soviet

<sup>96</sup> Ryan Haas, *Time to Rethink U.S. Trade Strategy in Asia*, Brookings Institution (Feb. 20, 2018) (online at <https://www.brookings.edu/blog/order-from-chaos/2018/02/20/time-to-rethink-u-s-trade-strategy-in-asia/>).

<sup>97</sup> Iren Yuan Sun, *The World's Next Great Manufacturing Center*, Harvard Business Review (May–Jun. 2017) (online at <https://hbr.org/2017/05/the-worlds-next-great-manufacturing-center>).

<sup>98</sup> Acha Leke, Mutsa Chironga, and Georges Desvaux, *Africa's Overlooked Business Revolution*, McKinsey Quarterly (Nov. 15, 2018) (online at <https://www.mckinsey.com/featured-insights/middle-east-and-africa/africas-overlooked-business-revolution>).

<sup>99</sup> *Id.*

<sup>100</sup> Eric Schmitt and Thomas Gibbons-Neff, *Russia Exerts Growing Influence in Africa, Worrying Many in the West*, New York Times (Jan. 28, 2020) (online at <https://www.nytimes.com/2020/01/28/world/africa/russia-africa-troops.html>).

<sup>101</sup> Pepe Zhang, *Belt and Road in Latin America: A Game Changer?*, Atlantic Council (Oct. 8, 2019) (online at <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/belt-and-road-in-latin-america-a-regional-game-changer/>).

<sup>102</sup> Lara Jakes, *As Protests in South America Surged, So Did Russian Trolls on Twitter, U.S. Finds*, New York Times (Jan. 19, 2020) (online at <https://www.nytimes.com/2020/01/19/us/politics/south-america-russian-twitter.html>).

<sup>103</sup> The Arctic Institute, *Russia* (Jun. 19, 2020) (online at <https://www.thearcticinstitute.org/countries/russia/>).

bases, along with its economic edict to control the Northern Sea Route, are harbingers of its intent to scoop up the Arctic on its quest to return to a global power.<sup>104</sup>

China for its part, is both partnering and competing with Russia in the Arctic.<sup>105</sup> In a formal white paper in 2018, China declared itself a near-Arctic state and laid out its priorities for the region.<sup>106</sup> While China's short-term interests appear commercial, its pursuance of scientific study, surveying, and mapping portend other intentions with military applications.<sup>107</sup>

## Exporting Soft Power

Strong offensive measures in the form of soft power initiatives protect vital U.S. interests by ensuring dialogue and enhanced cooperation. Humanitarian and economic aid programs foster good will and build civic capacity while also serving as a powerful check on the rise of authoritarian and autocratic influence. Exporting democracy through American projects and enterprises showcases democratic values such as human rights, personal liberties, and self-determination, all tenants that fail to thrive under authoritarian capitalism.

The American brand remains significantly stronger globally than most of its competitors, and the United States should both recognize and build on this advantage. The Chinese, by comparison, have significant branding issues, borne out of years of producing cheap goods often derived through unfair business practices. For all its seeming success, the Belt and Road Initiative has often caused the opposite of its intended effect: increased public distrust and apprehension by host nations due to an emphasis by China in establishing a debt relationship. Poorly constructed projects built by imported Chinese labor rather than local workers often go unfinished while many countries face buyer's remorse as they become mired in unsustainable debt from projects that cause environmental degradation and a decline in quality of life.<sup>108</sup>

Exporting American values by bolstering the State Department, United States Agency for International Development (USAID), and other American programs that promote transparency and human rights while growing democracy ameliorates global instability and reduces the potential for human conflict. History presages that when the United States competes from the moral high ground, it usually wins.

<sup>104</sup> Reuters, *'History is Repeating Itself': Russia Is Making Its Biggest Push into the Arctic Since the Soviet Union Fell*, Business Insider (Jan. 30, 2017) (online at <https://www.businessinsider.com/r-putins-russia-in-biggest-arctic-military-push-since-soviet-fall-2017-1>).

<sup>105</sup> Ling Guo and Steven Lloyd Wilson, *China, Russia and Arctic Geopolitics*, The Diplomat (Mar. 29, 2020) (online at <https://thediplomat.com/2020/03/china-russia-and-arctic-geopolitics/>).

<sup>106</sup> The State Council, The People's Republic of China, *China's Arctic Policy* (Jan. 26, 2018) (online at [http://english.www.gov.cn/archive/white\\_paper/2018/01/26/content\\_281476026660336.htm](http://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm)).

<sup>107</sup> Heljar Havnes and Johan Martin Seland, *The Increasing Security Focus in China's Arctic Policy*, The Arctic Institute (Jul. 16, 2019) (online at <https://www.thearcticinstitute.org/increasing-security-focus-china-arctic-policy/>).

<sup>108</sup> Wade Shepard, *How China's Belt and Road Became a 'Global Trail of Trouble'*, Forbes Magazine (Jan. 29, 2020) (online at <https://www.forbes.com/sites/wadeshepard/2020/01/29/how-chinas-belt-and-road-became-a-global-trail-of-trouble/#33b8ec89443d0>).

The United States should increase foreign leader engagements with non-traditional allies and seek to emphasize shared values and economic interests through soft power initiatives. As an example, when members of the Task Force visited Cambodia in early 2020, they were surprised to learn that it had been more than two years since a congressional delegation (CODEL) has visited the country. While many observers have determined that Cambodia may be lost to Chinese influence, members of the CODEL came to the tempered conclusion that even a small U.S. economic presence could garner a different outcome.

## **Military to Military**

The United States military, with its adherence to human rights and the rules of engagement, stands as the global model for how a free and open society should protect itself and its interests. Exporting U.S. values through military engagements, with both exercises and train and assist programs, builds trust and interoperability while increasing readiness, resiliency, and further protecting vital U.S. interests abroad.

Strengthening global partnerships through military to military relations allows the United States to maintain an agile forward footprint while bolstering the doctrine of credible deterrence.<sup>109</sup> Multi-national military exercises can increase resilience, interoperability and security cooperation. Successful examples abound throughout Asia, Africa, Europe, and the Western Hemisphere.

Also of great importance is the International Military Education and Training (IMET) program, where the return on investment is nearly incalculable. The State Department describes the IMET program, which trains foreign military personnel from allied nations, as a key element of U.S. security assistance.<sup>110</sup> With vigorous vetting and control measures to ensure adherence to human rights and the rule of law, the United States should strengthen the IMET program, which develops rapport and dialogue between U.S. and foreign military leaders while imparting American values and enhancing shared interests and security cooperation.

With thoughtful analysis and consideration, the United States should look to increase foreign military sales (FMS) to new partners with emerging economies. Increased FMS would allow the United States to strengthen its defense systems globally by boosting the flow of information and increasing interoperability. Because of the high demand for U.S. weapons systems, the United States can effectively influence foreign policy through security assistance programs.

## **Security Alliances and Nuclear Agreements**

Due to its agility and longevity, many historians regard the North Atlantic Treaty Association (NATO) as the most successful political alliance in history. Of the eight countries that made up its

<sup>109</sup> House Armed Services Committee, *Testimony of Michele Flournoy*, Theories of Victory-Innovative Concepts for National Security (Oct. 29, 2019) (online at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventId=110154>).

<sup>110</sup> Department of State, *Office of Security Assistance* (online at <https://www.state.gov/about-us-office-of-security-assistance/>).



former rival, the Warsaw Pact, seven eventually became part of NATO, while the eighth, the Soviet Union, was dismantled.<sup>111</sup> The alliance has given immense credence to the concept of credible deterrence as a tangible and viable option to bellicosity.

With the rise of Russian aggression, strengthening collective defense through the NATO alliance has become increasingly salient. But with three member nations, Turkey, Poland, and Hungary, trending away from democracy,<sup>112</sup> the alliance is becoming fraught with complexity. Still, the United States should reengage NATO and its member nations that adhere to democratic values and uphold human rights. In its 70-year history, Article 5 of the treaty, which states that an attack against one member shall be an attack against all, has been invoked only once, and it was on behalf of the United States following the 9/11 attacks. Since then, 1,052 non-American NATO troops have died in Afghanistan.<sup>113</sup>

The expansion of NATO, however, should be met with caution. Increasing membership without careful consideration could lead to the institution buckling under its own weight. For the alliance to remain meaningful, the underpinning of collective security must be adhered to, and members must be willing to fight on each other's behalf. Further expanding membership to countries on the Russia's border may also trigger a Russian redline.<sup>114</sup> It is also important to ensure equitable cost sharing in accordance with the principle of common funding to ensure the long-term financial health of the alliance.

Long-standing bilateral security agreements with Japan and South Korea, which hold considerable historical agency, also serve as prescient alliances in the wake of a rising China. A challenging dynamic, however, is the increasing animosity between Japan and South Korea over historical grievances and a trade war. The United States must work to assuage conflict between the rival nations to ensure stability on both the Korean Peninsula and in the greater Indo-Pacific region.

With a rapidly approaching expiration date, the United States and Russia should extend the highly successful Strategic Arms Reduction Treaty (New START) while negotiating a follow-on agreement.<sup>115</sup> The treaty significantly reduced the number of deployed nuclear warheads while also limiting the amount of launch vehicles the United States and Russia can deploy. With the dissolution of the Intermediate-Range Nuclear Forces (INF) Treaty, New START remains the only bilateral nuclear arms control agreement between the United States and Russia. Its lapse at a time when China and North Korea (and potentially Iran) are increasing their nuclear capabilities and arsenals

<sup>111</sup> Daniel Franklin, *How NATO is Shaping Up at 70*, The Economist (Mar. 14, 2019) (online at <https://www.economist.com/special-report/2019/03/14/how-nato-is-shaping-up-at-70>).

<sup>112</sup> Jonathan Katz and Torrey Taussig, *An Inconvenient Truth: Addressing Democratic Backsliding Within NATO*, Brookings Institution (Jul. 10, 2018) (online at <https://www.brookings.edu/blog/order-from-chaos/2018/07/10/an-inconvenient-truth-addressing-democratic-backsliding-within-nato/>).

<sup>113</sup> Icasualties.org (Apr. 2020) (online at <http://icasualties.org/>).

<sup>114</sup> Council on Foreign Relations, *Managing Global Disorder-Prospects for U.S. Russian Cooperation* (Aug. 23, 2017) (online at <https://www.cfr.org/report/managing-global-disorder-prospects-us-russian-cooperation>).

<sup>115</sup> Brian Sittlow, *New START: The Future of U.S.-Russian Arms Control*, Council on Foreign Relations (Jan. 28, 2020) (online at <https://www.cfr.org/in-brief/new-start-future-us-russia-nuclear-arms-control>).

would send a harmful message to adversaries and partners alike while further undermining the global Treaty on the Non-Proliferation of Nuclear Weapons (NPT).<sup>116</sup>

### **Statecraft vs. Warcraft**

When gaming out the future of defense, increasingly strained relations with China and the rising potential for conflict with Russia should remind the United States to consider diplomatic measures that adhere to the concept of statecraft versus the proliferation of war craft. Leveraging influence through economic, political, and social measures may be the most successful means of avoiding conflict while ensuring a stable, open, and transparent world order that allows democracies to thrive.

The United States remains China's largest trade partner, receiving 19 percent of its exports.<sup>117</sup> It also represents China's greatest trade surplus, at nearly \$300 billion for 2019.<sup>118</sup> Simply stated, China needs the United States economically, at least for the short term. And we have witnessed over the last year the challenges of the United States' reliance on Chinese goods and manufacturing. Still, as the United States reexamines its trade practice vulnerabilities and supply chain points of failure in the wake of the COVID-19 pandemic, it should also recognize and utilize its significant economic leverage with China.

Russia, for its part, may be more challenging to find short-term avenues for cooperation. A follow-on to the New START treaty, which serves Russian interests greatly, is an excellent starting point. Space exploration and other scientific study may be another.

<sup>116</sup> United Nations Office of Disarmament Affairs, *Treaty on the Non-Proliferation of Nuclear Weapons* (online at <https://www.un.org/disarmament/wmd/nuclear/npt/>).

<sup>117</sup> Central Intelligence Agency, *The World Fact Book: China* (online at <https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html>).

<sup>118</sup> Daniel Workman, *China's Top Trading Partners*, World's Top Exports (Jun. 18, 2020) (online at <http://www.worldstopexports.com/chinas-top-import-partners/>).

## SUPERCARGING THE INNOVATION BASE

A sophisticated array of technologies is emerging to transform society and alter the nature of warfare. The country that can develop and incorporate these technologies the fastest and most effectively will enjoy significant military and economic advantage for decades to come. The stakes are enormous, with many national security experts calling it a 21st century “Sputnik” moment. To meet this challenge and maintain military and economic advantage over strategic competitors like China and Russia, the United States must work to supercharge its innovation base.

The U.S. government and the Department of Defense (DOD) will need to better harness the innovative technology developed in the private sector, as private industry now far outpaces the U.S. government in overall investment in scientific research and development (R&D). The Pentagon must also adapt its culture and business practices to better support, and more quickly integrate, innovation from the private sector.

Historically, the United States has led the world in funding tech R&D, which has allowed it to maintain a strategic advantage. China, however, appears poised to challenge the United States as the overall leader in R&D spending.<sup>119</sup> In response, the U.S. government and the Pentagon should consider increasing investment in basic R&D and while developing R&D partnerships globally.

### DOD and Private Sector Innovation

Because the private sector generates much of the innovative technology the Pentagon will need to maintain the country’s military advantage, it is a national security imperative that the DOD continue to adapt its culture and business practices to bridge the divide between military and private sector partners to better incorporate emerging technologies. “Today, the private sector, not government, is developing the most critical technologies from which modern weapons systems are deriving the most significant advantage,” noted Eric Schmidt, the former chairman of Google.<sup>120</sup> Although the Pentagon can incorporate much from the private sector, it has a fundamentally different responsibility to protect the nation and make the investments to do so fairly and efficiently.

Pentagon culture and business practices are rightfully designed to be fair and open and to avoid waste and abuse. However, this can sometimes make them slower-moving, risk-averse, and process-based rather than outcome-based, which can hinder the military’s ability to fully utilize private sector innovation. Established practice and culture favor large, traditional business partners, which makes it more difficult for non-traditional companies with innovative technology to compete. The Pentagon knows how to acquire large programs of record like fighter jets or aircraft carriers, but it is less adept at purchasing at scale the types of emerging technologies that will be required for future conflict.

<sup>119</sup> John Sarget Jr., Marcy Gallo, and Moshe Schwartz, *The Global Research and Development Landscape and Implications of the Department of Defense*, Congressional Research Service (Nov. 8, 2018) (online at <https://fas.org/sgp/crs/natsec/R45403.pdf>).

<sup>120</sup> House Committee on Armed Services, Testimony of Dr. Eric Schmidt, *Hearing on Promoting DOD’s Culture of Innovation* (Apr. 17, 2018) (online at <https://docs.house.gov/meetings/AS/AS00/20180417/108132/HHRG-115-AS00-Wstate-SchmidtE-20180417.pdf>).

To mitigate risk and prevent exploitation, the military often prioritizes consensus and process at the expense of speed. Because of risk aversion and fear of potential failure, the Pentagon often fails to fully utilize its existing authorities to quickly incorporate private sector technology, even when urgently necessary. This hinders its ability to fully leverage outside advances at the necessary speed and scale.

In terms of business practices, the Pentagon's acquisition process is lengthy and designed to minimize risk and ensure competition and fairness; however, this often leads it to default to legacy platforms rather than the emerging technology-based systems necessary to operate in future conflicts. As a result, too many companies that develop critical technology succumb to the "valley of death," the gap between a technology's development and the Pentagon's decision to support it with a program of record.

When it does support non-traditional companies, the DOD often focuses on early stage investments at the expense of later stage engagement that would allow a company to grow at scale.<sup>121</sup> Often, and for valid reasons, the Pentagon makes a number of small bets on a variety of companies but is seemingly less inclined to wager on nontraditional companies by providing them contracts for programs of record at scale, even when the technology has been validated and fits a military requirement. This reticence makes it more difficult for innovative companies that want to partner with the DOD to obtain private sector funding.

When the Pentagon grants a contract, it signals to other investors that the company is worthy of investment.<sup>122</sup> Without long-term commitment, however, smaller innovative companies with essential technology are often forced away due to the need to demonstrate growth more quickly than the Pentagon can award a contract.

According to a report by the Government Accountability Office (GAO), the complexity of the acquisition process and unstable budget environment are consistent impediments to non-traditional companies that partner with the DOD. The lengthy contracting timeline, government-specific requirements, and concerns with intellectual property rights further frustrate private entities. These barriers drive away otherwise willing companies that instead pursue avenues where the cost to compete is lower and decisions are made faster.<sup>123</sup>

## **Pentagon Innovation**

Currently, the Pentagon is sponsoring multiple groundbreaking programs that foster and integrate innovation and technology developed in the private sector. Initiatives like the Defense

<sup>121</sup> Ronald Reagan Institute, *The Contest for Innovation: Strengthening America's National Security Innovation Base in an Era of Strategic Competition*, Report of the Task Force on 21<sup>st</sup>-Century National Security Technology and Workforce (2019) (online at [https://www.reaganfoundation.org/media/355498/the\\_contest\\_for\\_innovation\\_report.pdf](https://www.reaganfoundation.org/media/355498/the_contest_for_innovation_report.pdf)).

<sup>122</sup> House Committee on Armed Services, *Testimony of Raj Shah, Future of Defense Task Force Hearing on Supercharging the Innovation Base* (Feb. 5, 2020) (online at <https://armedservices.house.gov/2020/2/future-of-defense-task-force-hearing-supercharging-the-innovation-base>).

<sup>123</sup> Government Accountability Office, *DOD Is Taking Steps to Address Challenges Faced by Certain Companies* (Jul. 2017) (online at <https://www.gao.gov/assets/690/686012.pdf>).

Innovation Unit (DIU), and Air Force's AFWERX and Kessel Run, provide critical capability and have proven successful, but they are currently too small to leverage private sector technology and innovation at the necessary scale. However, the establishment of new models, such as AFVentures, to attract greater private sector investment to defense technologies have shown value and should be closely examined for their effectiveness in rebalancing the national security innovation ecosystem.

The Pentagon's outreach in places like Boston, Silicon Valley, and Austin has been successful, but more needs to be done in these areas and around the country. There are innovative companies, universities, and thought leaders throughout the United States that would welcome the opportunity to work with the DOD. But the Pentagon has so far only been able to tap into a fraction of the innovation being developed in the United States.

Successful DOD programs for engagement and innovation include the Defense Advanced Research Projects Agency (DARPA), which has a storied history of developing and supporting breakthrough technologies, including some of the country's foundational advancements. The Pentagon should continue to use it as a model for innovation. By effectively employing basic scientific R&D funding, DARPA has helped develop multiple game-changing technologies, including stealth, the internet, and personal electronics, all of which have benefited both the military and the private sector.

The DARPA model incorporates a relatively flat hierarchy that grants its program managers significant latitude and flexibility to develop innovative ideas. DARPA also has flexible acquisition and hiring authorities, which allows the DOD to engage unique organizations. And although its overall funding has remained relatively flat, DARPA continues to attract talented employees, foster critical relationships with innovative, non-traditional DOD partners, and develop and incorporate critical technologies.<sup>124</sup> Further, DARPA has long served as an ambassador on behalf of the military to a variety of organizations, which has helped reduce the cultural gap between the Pentagon and potential partners.

## **Cultural Divide Between the Pentagon and the Private Sector**

While many companies and universities consider it patriotic to partner with the military, some organizations and individuals are reluctant to work with the DOD for ethical reasons. As a much-discussed example, in 2018, Google stepped away from Project Maven, a Pentagon artificial intelligence (AI) project, due to ethical concerns of some of its employees. Still, Google continues to partner with the DOD on other projects, as do many other large and small technology companies. And many institutions and their members view partnering with the Pentagon as a potential opportunity for service, funding, and growth.

Typically, organizations choose not to partner with the Pentagon because of frustrating business practices rather than ethical reticence. There is a cultural divide between the military and

<sup>124</sup> Congressional Research Service, *Defense Advanced Research Projects Agency: Overview and Issues for Congress* (Mar. 17, 2020) (online at <https://fas.org/sgp/crs/natsec/R45088.pdf>).

private industry, but this divide is based primarily on comfort with risk, speed of decisions, business practices, and incentives.

Bridging the cultural divide and improving the Pentagon's ability to leverage private sector innovation and technology is a national security imperative because private industry, rather than the U.S. government, is now the primary developer of the technology underpinning U.S. military technology.

## **Department of Defense Research and Development Funding**

Pentagon investment in basic scientific R&D is critical to maintaining the military's technological advantage by supporting game-changing technological breakthroughs. In 1960, DOD R&D alone accounted for 36 percent of global R&D spending, but by 2016, it had fallen to less than 4 percent.<sup>125</sup> And within its current R&D budget, the Pentagon is spending less on the basic foundational research historically used to develop new technologies.

Basic R&D spending, such as that found in the Defense Science and Technology account, is considered technological "seed corn" because of the insights that often emerge from it.<sup>126</sup> The goal of basic defense research funding is to acquire new knowledge that enhances and transforms future capabilities. DOD basic research has historically invested in high-risk endeavors and was the first to support many of the world's leading scientists and engineers at universities, federal laboratories, and in the private sector on a variety of revolutionary technologies.<sup>127</sup>

Funding for this type of basic foundational defense R&D, however, has remained relatively flat in recent years.<sup>128</sup> Instead, the Pentagon has increasingly focused on adapting technology for more near-term defense applications, which could leave a critical gap in creating new breakthrough technologies often found throughout the military's research and university enterprise.

The Pentagon has long relied on technology developed from its defense laboratory enterprise at places like the Air Force Research Laboratory, Army Research Laboratory, and the Office of Naval Research. The military sponsors a variety of federally funded R&D centers (FFRDCs), including the Institute for Defense Analyses and the Lincoln Laboratory, which provide critical research and technological development.<sup>129</sup>

The Pentagon also supports university-affiliated research centers at places like the Johns Hopkins University Applied Physics Laboratory that help develop and incorporate emerging

<sup>125</sup> John Sargent Jr. and Marcy Gallo, *The Global Research and Development Landscape and Implications for the Department of Defense*, Congressional Research Service (Nov. 8, 2018) (online at <https://crsreports.congress.gov/product/pdf/R/R45403>).

<sup>126</sup> John Sargent Jr., *Defense Science and Technology Funding*, Congressional Research Service (Feb. 21, 2018) (online at <https://fas.org/sgp/crs/natsec/R45110.pdf>).

<sup>127</sup> Department of Defense, *Report of the Task Force on Basic Research*, Defense Science Board (Jan. 2012) (online at <https://fas.org/irp/agency/dod/dsb/basic.pdf>).

<sup>128</sup> John Sargent Jr., *Defense Science and Technology Funding*, Congressional Research Service (Feb. 21, 2018) (online at <https://fas.org/sgp/crs/natsec/R45110.pdf>).

<sup>129</sup> Government Accountability Office, *Defense Science and Technology: Action Needed to Enhance Use of Lab Initiated Research Authority* (Dec. 2018) (<https://www.gao.gov/assets/700/696192.pdf>).

technologies and counter rising threats. Further, the DOD provides a significant funding to universities for similar purposes, and support for colleges and universities accounts for roughly half of its basic research budget.<sup>130</sup>

DOD investment in basic R&D funding has historically proven extremely successful, and the work done by the Pentagon's laboratories and university partners is a critical component of the United States' technological and military advantage. And although the private sector continues to outpace government-supported R&D, it cannot replace the government-funded basic R&D that has historically fueled the United States' economic and military advantage.

### **Private Sector Research and Development Funding**

The U.S. government is no longer the primary funder of R&D in the United States or the world, as private industry now far outpaces the U.S. government's R&D spending.<sup>131</sup> And while private sector R&D is essential for a healthy economy, it is not a replacement for the type of foundational R&D the United States needs to remain competitive in the defense realm.

Private sector research often focuses on shorter-term development and the commercialization of existing technology rather than basic foundational research to develop wholly new knowledge and technology.<sup>132</sup> A recent GAO report found that in past years, defense contractors put only 40 percent of their independent research funding towards DOD priority areas such as AI, autonomy, hypersonic weapons, and directed energy.<sup>133</sup>

Also at issue is the understanding that military technology may not have a clear private sector application, which limits private sector investment. Still, the Pentagon must increasingly leverage the private sector to develop the technology required to maintain the United States' technological and economic advantage over its strategic competitors.

Of concern to the Task Force is the notion that the gap between the United States and its competitors is narrowing sharply. Working within the concept of military-civil fusion, China is blurring the lines between the government, academia, and private industry, taking an aggressive, whole-of-government approach to develop and leverage emerging technologies for economic and military advantage. The United States and its innovation base are competing against a country that can employ a long-term and top-down plan that can seize innovation wherever it occurs.<sup>134</sup> To

<sup>130</sup> John Sargent Jr., *Federal Research and Development (R&D) Funding: FY2020*, Congressional Research Service (Mar. 18, 2020) (online at <https://fas.org/sgp/crs/misc/R45715.pdf>).

<sup>131</sup> Congressional Research Service, *U.S. Research and Development Funding and Performance: Fact Sheet* (Jan. 2020) (online at <https://fas.org/sgp/crs/misc/R44307.pdf>).

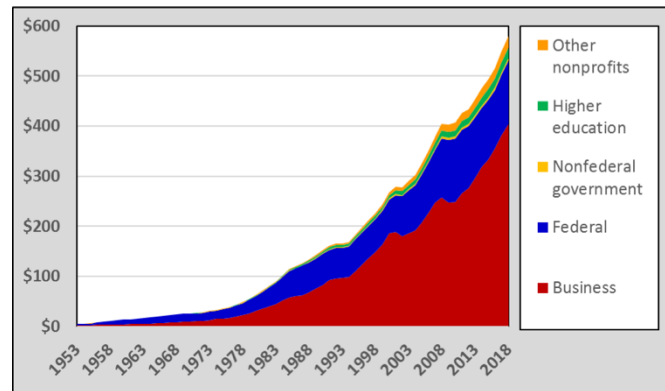
<sup>132</sup> Ronald Reagan Institute, *The Contest for Innovation: Strengthening America's National Security Innovation Base in an Era of Strategic Competition*, Report of the Task Force on 21<sup>st</sup> Century National Security Technology and Workforce (2019) (online at [https://www.reaganfoundation.org/media/355498/the\\_contest\\_for\\_innovation\\_report.pdf](https://www.reaganfoundation.org/media/355498/the_contest_for_innovation_report.pdf)).

<sup>133</sup> *Id.*

<sup>134</sup> Ronald Reagan Institute, *The Contest for Innovation: Strengthening America's National Security Innovation Base in an Era of Strategic Competition*, Report of the Task Force on 21<sup>st</sup> Century National Security Technology and Workforce (2019) (online at [https://www.reaganfoundation.org/media/355498/the\\_contest\\_for\\_innovation\\_report.pdf](https://www.reaganfoundation.org/media/355498/the_contest_for_innovation_report.pdf)).

remain competitive, the United States and the DOD must quickly adapt. While the United States still spends more in total R&D than China, Chinese private sector and government investment is increasing more rapidly than similar U.S. outlays.

### U.S. R&D Expenditures by Source of Funding, 1953–2018<sup>135</sup>



**Source:** CRS analysis of National Science Foundation, *National Patterns of R&D Resources: 2017–18 Data Update*, NSF 20-307, Table 6, January 8, 2020, <https://nces.nsf.gov/pubs/nsf20307>.

In fact, China recently overtook the United States in overall private sector R&D spending and continues to increase its government-supported R&D.<sup>136</sup> These trends have significant implications for the United States’ technological advantage as China aggressively closes the gap and U.S. government-funded R&D decreases.

### Total U.S. Research and Development Funding

Historically, the United States has outpaced every other country combined in overall R&D spending, but its lead is quickly diminishing. Over the past two decades, China has rapidly increased its investment in overall R&D, while U.S. spending rates have lagged. Today, the United States still spends more than any other country, but China is on track to take the lead in global R&D spending by 2030 if current trends continue.<sup>137</sup>

In 1960, the United States accounted for 69 percent of the world’s R&D spending. In 2017, it was 28 percent.<sup>138</sup> By comparison, between 2010 and 2017, China boosted its overall investment

<sup>135</sup> Congressional Research Service, *U.S. Research and Development Funding and Performance: Fact Sheet* (Jan. 2020) (online at <https://fas.org/sgp/crs/misc/R44307.pdf>).

<sup>136</sup> Govini, *America’s Eroding Technological Advantage: National Defense Strategy RDT&E Priorities in an Era of Great-Power Competition with China* (online at [https://www.govini.com/wp-content/uploads/2020/02/Govini\\_NDS-Priorities-RDTE.pdf?utm\\_source=web&utm\\_medium=direct&utm\\_campaign=RDTE](https://www.govini.com/wp-content/uploads/2020/02/Govini_NDS-Priorities-RDTE.pdf?utm_source=web&utm_medium=direct&utm_campaign=RDTE)).

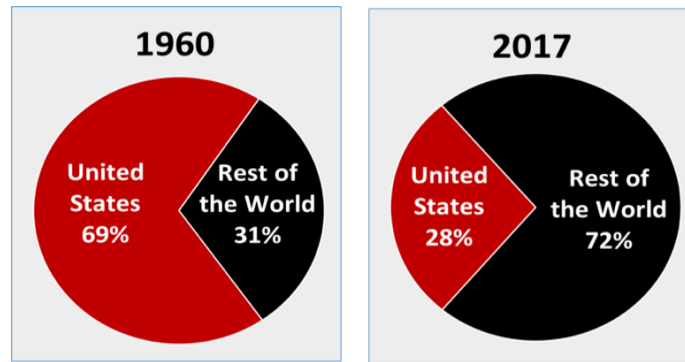
<sup>137</sup> Council on Foreign Relations, *Innovation and National Security: Keeping Our Edge* (2019) (online at [https://www.cfr.org/report/keeping-our-edge/pdf/TFR\\_Innovation\\_Strategy.pdf](https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf)).

<sup>138</sup> Congressional Research Service, *Global Research and Development Expenditures: Fact Sheet* (Sept. 2019) (online at <https://fas.org/sgp/crs/misc/R44283.pdf>).

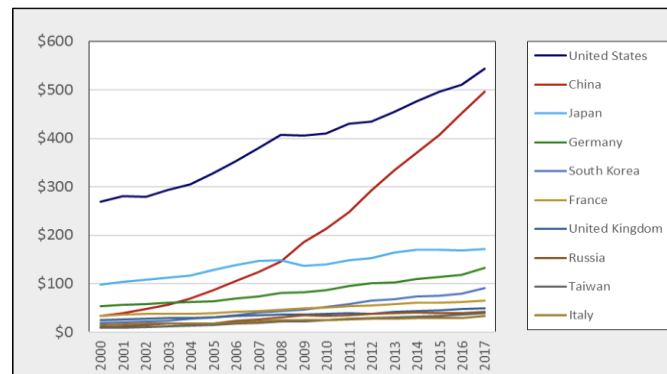


from roughly \$200 billion to nearly \$500 billion. In the past two decades, Chinese investment in R&D has increased by nearly 1,400 percent, while spending rates in the United States have remained relatively steady.<sup>139</sup>

#### U.S. Share of Global R&D<sup>140</sup>



#### R&D Expenditures of Selected Countries, 2000–2017<sup>141</sup>

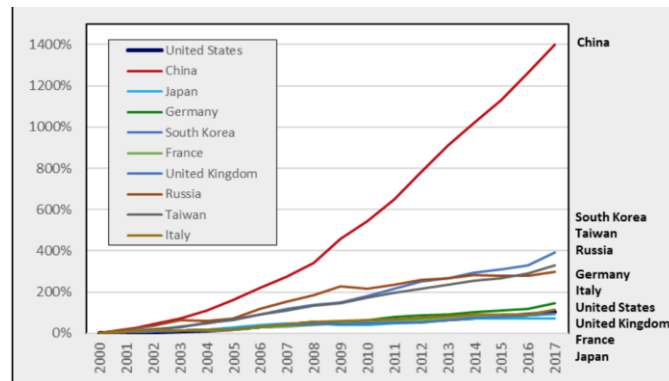


<sup>139</sup> *Id.*

<sup>140</sup> *Id.*

<sup>141</sup> *Id.*

## Growth in R&D Expenditure Since 2000 for Selected Countries, 2000–2017<sup>142</sup>



Source: CRS analysis of Organization for Economic Development and Cooperation, OECD.Stat database, [https://stats.oecd.org/Index.aspx?DataSetCode=MSTI\\_PUB](https://stats.oecd.org/Index.aspx?DataSetCode=MSTI_PUB)

### Global Partnerships to Leverage Innovation

As China continues to substantially increase its investment in R&D and strengthen its innovation base, technological alliances with security partners will be critical for the United States to maintain its strategic advantage. In addition to utilizing its innovation base, the United States can support and incorporate technology developed in other countries while fostering these partnerships.<sup>143</sup>

Similar to security and military relationships, collective science and technology alliances are critical to long-term competitiveness since many U.S. partners are developing critical innovative technology.<sup>144</sup> Most of these countries have a vested interest in ensuring the distribution of the technology they have developed is reflective of their values. Ideally, the United States and its partners would responsibly collaborate to share technological innovation and R&D while developing common technological standards.

The regulatory structure of the United States, however, sometimes creates barriers to technology and research exchanges with key allies.<sup>145</sup> It is important to protect sensitive proprietary technology, but that goal should be balanced with the need to leverage the talent and technology developed by international partners. Thoughtful policy will allow the United States to protect its critical technology while leveraging and supporting the innovation of its partners and allies.

<sup>142</sup> *Id.*

<sup>143</sup> Council on Foreign Relations, *Innovation and National Security: Keeping Our Edge* (2019) (online at [https://www.cfr.org/report/keeping-our-edge/pdf/TFR\\_Innovation\\_Strategy.pdf](https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf)).

<sup>144</sup> *Id.*

<sup>145</sup> Ronald Reagan Institute, *The Contest for Innovation: Strengthening America's National Security Innovation Base in an Era of Strategic Competition*, Report of the Task Force on 21<sup>st</sup> Century National Security Technology and Workforce (2019) (online at [https://www.reaganfoundation.org/media/355498/the\\_contest\\_for\\_innovation\\_report.pdf](https://www.reaganfoundation.org/media/355498/the_contest_for_innovation_report.pdf)).

## Protecting the Industrial Base

Competitor countries, most notably China, are attacking the U.S. defense industrial base to steal valuable intellectual property and capability. Former Director of the National Security Agency General Keith Alexander estimated that as early as 2012, the United States was losing a quarter of \$1 trillion each year to industrial espionage, primary originating from China. He called it “the greatest transfer of wealth in history.”<sup>146</sup> This theft of intellectual property puts the United States at a significant disadvantage militarily and economically as competitors obtain parity in capability without having to spend the time and resources to develop it.

To reverse this trend, government leaders and the private sector must protect the United States’ innovation base from theft and ensure its resiliency to withstand deliberate attacks and disruptions.

## Domestic Manufacturing

Much of the United States’ manufacturing supply chain is now vulnerable to single points of failure. This breakdown has significant national security and economic implications, as the COVID-19 pandemic acutely highlighted. For example, 80 percent of the ingredients to make medicines and 97 percent of antibiotics in the United States come from China.<sup>147</sup>

A recent review by the Brookings Institution found that the destruction of America’s industrial capacity has become “the single biggest unacknowledged threat to our national security,” as globalization has moved the United States’ manufacturing base abroad.<sup>148</sup> In addition to manufacturing capability, the United States has become over-reliant on raw materials from overseas, including essential defense materials. China is further increasing its global control of rare earths, which are a critical component of many weapons systems, to include fighter jets and munitions.<sup>149</sup>

The United States must address these vulnerabilities by investing in domestic supply chains and American manufacturing to make it less beholden to foreign countries, including potential adversaries.

<sup>146</sup> Josh Rogin, *NSA Chief: Cybercrime Constitutes the “Greatest Transfer of Wealth in History”*, Foreign Policy (Jul. 9, 2012) (online at <https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>).

<sup>147</sup> Michael Brown, Eric Chewing, and Pavneet Singh, *Preparing the United States for the Superpower Marathon with China*, Brookings Institution (Apr. 2020) (online at <https://www.brookings.edu/research/preparing-the-united-states-for-the-superpower-marathon-with-china/>).

<sup>148</sup> *Id.*

<sup>149</sup> Jeffery Green, *What Will the U.S. Defense Industry Do When China Cuts Off Rare Earth Supplies?*, Defense News (Jul. 5, 2019) (online at <https://www.defensenews.com/opinion/commentary/2019/07/05/what-will-the-us-defense-industry-do-when-china-cuts-off-rare-earth-supplies/>).



## DEVELOPING A 21<sup>ST</sup> CENTURY WORKFORCE

To maintain its strategic advantage, the United States must recruit and develop a workforce with the requisite skills and talent to maintain the country's technological and military advantage. In matters of national security, people are more important than hardware; therefore, the United States must develop, recruit, and retain the most talented science and technology, military, and national security professionals globally.

Along with recruiting and growing science, technology, engineering, and mathematics (STEM) talent, the military and national security community must update personnel policies to ensure that they can attract and foster talent.

### STEM Talent

STEM talent and education are the fundamental building blocks of the technological innovation necessary to maintain the United States' strategic advantage. In testimony before the Task Force, Raj Shah stated that "The United States' innovation superpower over the past half-century has been its investment in human capital."<sup>150</sup> While the United States has long had an advantage due to its investment in STEM education, its preeminence is at risk as global competitors rush to catch up. To maintain its lead, the United States must grow STEM talent at home and aggressively recruit it from abroad.

Early STEM education is paramount. Former Commander of U.S. Special Operations Admiral William McRaven argues that the need to improve the quality of Pre-K through Grade 12 education is the greatest national security issue facing the United States.<sup>151</sup> A National Science Foundation report recently found, however, that the United States is failing to provide quality elementary and secondary mathematics and science education for all students. Eighth-grade students in the United States placed ninth in mathematics and science out of 19 developed countries in 2015. (Notably, Russia outpaced the United States, while it appears that China did not participate in the analysis.)<sup>152</sup>

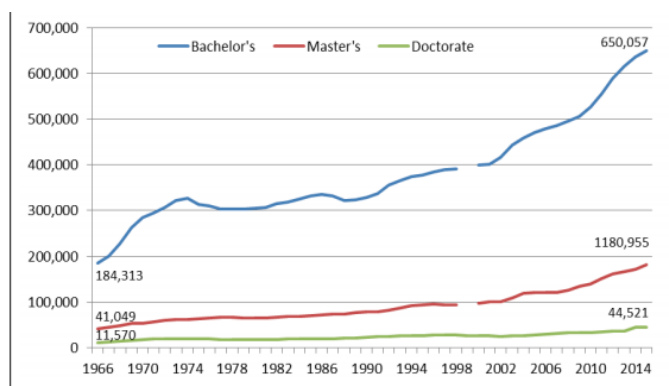
While the total number of American students graduating with STEM degrees in the United States (along with the number of overall college graduates) is rising, the country is not producing the amount of homegrown STEM talent required to maintain its technological, military, and economic advantage.

<sup>150</sup> House Committee on Armed Services, *Testimony of Raj Shah, Future of Defense Task Force Hearing: Supercharging the Innovation Base* (Feb. 5, 2020) (online at <https://armedservices.house.gov/2020/2/future-of-defense-task-force-hearing-supercharging-the-innovation-base>).

<sup>151</sup> Shannon Najmabadi, *Chancellor Bill McRaven on higher education, his time at the UT System and what's next*, The Texas Tribune (May 29, 2018) (online at <https://www.texastribune.org/2018/05/29/bill-mcraven-ut-system-chancellor-texas-higher-education/>).

<sup>152</sup> National Science Board, *Science and Engineering Indicators: Elementary and Secondary Mathematics and Science Education* (Sept. 2019) (online at <https://nces.nsf.gov/pubs/nsb20196/executive-summary>).

## Number of S&E Degrees Awarded from 1966 to 2015, by Degree Level<sup>153</sup>



**Source:** National Science Foundation, National Center for Science and Engineering Statistics, "Table 1," *Science and Engineering Degrees: 1966-2012*, NSF 15-326, June 2015; IPEDS Completions from webCASPAr at <https://ncesdata.nsf.gov/webcaspar/>.

As a singular example, U.S. universities will only educate 30 percent of the graduates necessary to fill computer specialist job opportunities in the United States.<sup>154</sup> Further exacerbating this low number is the fact that women and minorities are severely underrepresented in the STEM fields in the United States.<sup>155</sup> Women make up only 28 percent of the science and engineering workforce. And only 2.2 percent of Latinos, 2.7 percent of African Americans, and 3.3 percent of American Indians and Alaska Natives have earned a degree in STEM.<sup>156</sup> When gaming out the future of defense, the United States must seek to leverage the capabilities of all of its citizens.

The United States must also increase its retention of foreign talent. In 2017, foreign-born students accounted for 54 percent of master's degrees and 44 percent of doctorate degrees awarded in STEM fields in the United States.<sup>157</sup> Notably, China sends the most STEM students to the United States, with India a close second.<sup>158</sup> When these foreign-born students return to their home countries, they take with them critical knowledge and capacity. And while some want to return to their home countries, many choose to stay in the United States if allowed. The U.S. must recognize this immigration shortfall by aggressively expanding visas for STEM talent.

<sup>153</sup> Boris Granovskiy, *Science, Technology, Engineering, and Mathematics (STEM) Education: An Overview*, Congressional Research Service (Jun. 12, 2018) (online at <https://fas.org/sgp/crs/misc/R45223.pdf>).

<sup>154</sup> Council on Foreign Relations, *Innovation and National Security: Keeping Our Edge* (2019) (online at [https://www.cfr.org/report/keeping-our-edge/pdf/TFR\\_Innovation\\_Strategy.pdf](https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf)).

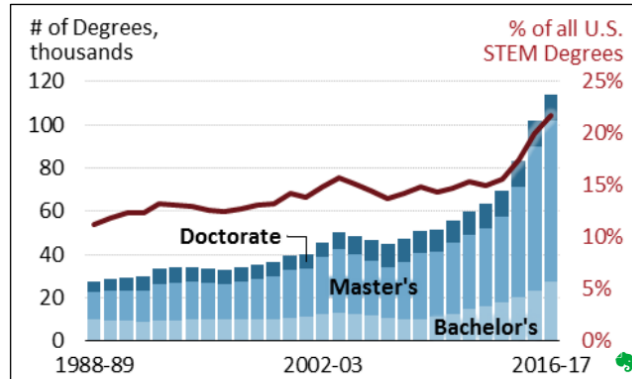
<sup>155</sup> Boris Granovskiy, *Science, Technology, Engineering, and Mathematics (STEM) Education: An Overview*, Congressional Research Service (Jun. 12, 2018) (online at <https://fas.org/sgp/crs/misc/R45223.pdf>).

<sup>156</sup> Council on Foreign Relations, *Innovation and National Security: Keeping Our Edge* (2019) (online at [https://www.cfr.org/report/keeping-our-edge/pdf/TFR\\_Innovation\\_Strategy.pdf](https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf)).

<sup>157</sup> Congressional Research Service, *Foreign STEM Students in the United States* (Nov. 1, 2019) (online at <https://crsreports.congress.gov/product/pdf/IF/IF11347>).

<sup>158</sup> *Id.*

## STEM Degrees Earned by Foreign Students<sup>159</sup>



**Source:** CRS display of data from U.S. Department of Education, National Center for Education Statistics, Integrated Postsecondary Education Data System.

The quantifiable success of recent immigrants is staggering. Nearly half of all Fortune 500 companies in the United States, valued collectively at \$5.3 trillion in 2017, were started by first- or second-generation Americans.<sup>160</sup> It is also important to note that, according to the National Science Foundation, 72 percent of foreign doctoral students were still in the United States 10 years after earning their degrees, including 90 percent of Chinese students.<sup>161</sup>

Still, immigration policy is hindering the United States' ability to attract and retain top foreign STEM talent that instead flows to other countries, including competitors. This occurs even as American companies, many from the military industrial base, have asserted that they need additional STEM talent from abroad to grow and help the United States maintain its economic and technological advantage.<sup>162</sup>

To compete, the United States must not only produce and attract STEM talent but also incorporate it in the national security apparatus. The lengthy hiring and clearance process hinders the ability of both the U.S. government and many U.S. companies to leverage top STEM talent. Therefore, programs such as Hacking for Defense that create pathways for talented students to work in national security should be expanded.

Similarly, opportunities for STEM students to obtain security clearances while still pursuing their education should be expanded. This innovative process would allow for select participants to begin both the clearing and visa processes in graduate school so they are ready to start work upon

<sup>159</sup> *Id.*

<sup>160</sup> Ian Hathway, *Almost half of Fortune 500 Companies were founded by American immigrants or their children*, Brookings Institution (Dec. 2017) (online at <https://www.brookings.edu/blog/the-avenue/2017/12/04/almost-half-of-fortune-500-companies-were-founded-by-american-immigrants-or-their-children/>).

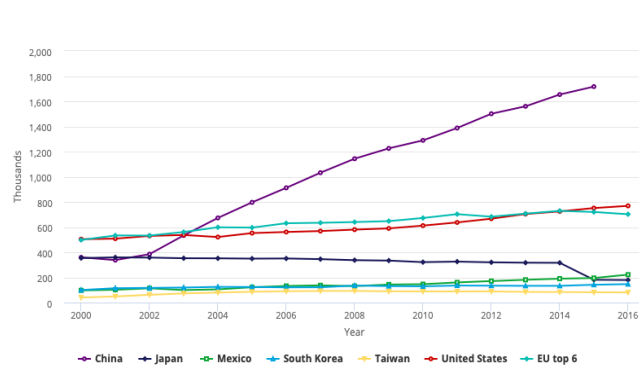
<sup>161</sup> Congressional Research Service, *Foreign STEM Students in the United States* (Nov. 1, 2019) (online at <https://crsreports.congress.gov/product/pdf/IF/IF11347>).

<sup>162</sup> Council on Foreign Relations, *Innovation and National Security: Keeping Our Edge* (2019) (online at [https://www.cfr.org/report/keeping-our-edge/pdf/TFR\\_Innovation\\_Strategy.pdf](https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf)).

graduation. In addition, the United States should create scholarships and incentives for STEM students and graduates to work in national security, including a dedicated commissioning source for military officers with science and technology skills. These types of initiatives will be critical as competitors of the United States seek to develop their own STEM talent.

While U.S. investment has remained relatively flat, China is aggressively investing in STEM education. In 2015, China produced more than 1.7 million science and engineering first degrees (equivalent to a U.S. undergraduate degree), while the United States produced about 750,000 the following year.<sup>163</sup>

### First University Degrees in S&E, by Selected Region, Country, or Economy: 2000–2016<sup>164</sup>



China is also aggressively investing in universities, research, and academic publications, and while the quality of Chinese STEM education still lags the United States, it is rapidly advancing. China is further recruiting STEM talent globally through its Thousand Talents Program, where it offers foreign scientists sizeable salaries and budgets to conduct research. Notably, the founder of Huawei asserted that the company would be happy to bring in foreign STEM talent unable to work in the United States.<sup>165</sup>

The Chinese government has engaged some of its citizens in the United States to steal valuable technology, and the United States must do more to protect its intellectual property and aggressively punish perpetrators. In October 2018, the secretary of defense announced the formation of the Protecting Critical Technology Task Force to prevent the loss of classified and unclassified information that is placing the Department's investments at risk and eroding the lethality and survivability of our forces.

Immigrants in the STEM fields have long been crucial to the United States' military and economic prowess, and American researchers and innovators are hindered if they are unable to collaborate and work alongside top talent from other countries. In fact, the United States has long

<sup>163</sup> National Science Board, *The State of U.S. Science and Engineering 2020* (Jan. 2020) (online at <https://ncses.nsf.gov/pubs/nsb20201/u-s-and-global-education#k-12-mathematics-and-science>).

<sup>164</sup> *Id.*

<sup>165</sup> Time Magazine, *Trump's Trade War Targets Chinese Students at Elite U.S. Schools* (Jun. 2019) (online at <https://time.com/5600299/donald-trump-china-trade-war-students/>).



enjoyed a security advantage in part because of the contributions of immigrants to programs like the Manhattan Project and the Mercury and Apollo space programs, which shaped the world order in favor of the United States. These successes are why Congress should create a National Security Innovation Base Visa that would provide an expedited pathway for highly skilled and vetted foreign students and workers to stay in the United States and contribute to the nation's security and innovation base.<sup>166</sup>

Developing homegrown STEM talent and recruiting it from abroad is a national security imperative for the United States, particularly as countries like China aggressively invest in STEM talent with a plan to overtake the United States.

## **Military Talent**

To maintain its competitive advantage, the United States must modernize its personnel system to recruit, retain, and promote military talent. "Winning the unpredictable next war will be less about advanced war machines and silicon chips than about out-thinking the enemy, and having a force chock-full of bright, adaptive leaders who can quickly navigate complex problems under the intense time pressures of modern combat," according to authors Ret. Lt. Gen. David Barno and Dr. Nora Bensahel.<sup>167</sup>

Military personnel policies, however, have not evolved to effectively recruit and retain people with these abilities. A recent report from the Center for New American Security found that, although the speed of conflict has increased exponentially, the military personnel system essentially runs the way it did in the mid-20<sup>th</sup> century.<sup>168</sup> It is slow-moving, rigid, and frequently fails to incentivize and promote innovative service members.<sup>169</sup>

Too often, the military personnel system takes a one-size-fits-all approach. While many service members increasingly want to influence their career trajectory, many are on a rigid career track that punishes any deviation, even if an assignment would benefit the service member and the military.<sup>170</sup> Many contend the system is blind to merit with little room for promotion based on ability and past performance, and even those with exceptional skill and talent are generally promoted at the same time as their peers. This not only wastes critical talent, but it

<sup>166</sup> Ronald Reagan Institute, *The Contest for Innovation: Strengthening America's National Security Innovation Base in an Era of Strategic Competition*, Report of the Task Force on 21<sup>st</sup> Century National Security Technology and Workforce (2019) (online at [https://www.reaganfoundation.org/media/355498/the\\_contest\\_for\\_innovation\\_report.pdf](https://www.reaganfoundation.org/media/355498/the_contest_for_innovation_report.pdf)).

<sup>167</sup> David Barno and Nora Bensahel, *Can the U.S. Military Halt Its Brain Drain?* The Atlantic (Nov. 5, 2015) (online at <https://www.theatlantic.com/politics/archive/2015/11/us-military-tries-halt-brain-drain/413965/>).

<sup>168</sup> Phillip Carter, Katherine Kidder, Amy Schafer, and Andrew Swick, *AVF 4.0: The Future of the All-Volunteer Force*, Center for New American Security (Mar. 2017) (online at <https://www.cnas.org/publications/reports/avf-4-0-the-future-of-the-all-volunteer-force>).

<sup>169</sup> David Barno and Nora Bensahel, *Can the U.S. Military Halt Its Brain Drain?*, The Atlantic (Nov. 5, 2015) (online at <https://www.theatlantic.com/politics/archive/2015/11/us-military-tries-halt-brain-drain/413965/>).

<sup>170</sup> Phillip Carter, Katherine Kidder, Amy Schafer, and Andrew Swick, *AVF 4.0: The Future of the All-Volunteer Force*, Center for New American Security (Mar. 2017) (online at <https://www.cnas.org/publications/reports/avf-4-0-the-future-of-the-all-volunteer-force>).

also drives away high-performing service members who are seeking faster and more meritorious advancement.

Moreover, the current system is designed for a continuous military career track that often fails to allow for breaks in service to develop skills, pursue higher education, or account for personal responsibilities like starting a family or caring for aging relatives. Save for a few exceptions, the system has limited ability to incorporate mid- and senior-level recruits, even those with high-demand skills. Service members increasingly want flexibility and control in their careers to both capitalize on experience and prepare for their professional and personal futures outside the military.

Many of the best leaders are choosing to leave the military, citing the rigid and bureaucratic personnel system.<sup>171</sup> This system applies to nearly every service member, regardless of rank or position. In recent years, many transitioning service members have also pointed to their frustration not with multiple combat deployments but with the staggering sacrifice to pursue ill-defined and seemingly unattainable strategic objectives. This departure of talent hurts the military in both the short and long term.<sup>172</sup>

The changing nature of warfare dictates that the modern U.S. military will need an increasing number of service members with the ability to operate in a complex and fast-moving battlespace with limited communication or direction from higher authority. In addition to combat leadership skills, the military must attract and promote service members with the intellectual acumen to develop the strategic and operational concepts necessary to deter conflict and win in the future.

While the U.S. military personnel system produces outstanding leaders, it must grow its ability to produce more service members with expanded characteristics and capabilities to meet emerging threats. History has repeatedly shown that technological superiority does not guarantee victory and that new ways of thinking can be more powerful than new weapons. Future leaders and strategists will need to understand emerging warfighting concepts like joint and multidomain warfare. They will further need a comprehensive understanding of national power and how to integrate military tools into a whole-of-government effort.

Military instruments alone will be insufficient. Future military leaders must apply and integrate all aspects of national power, including economic, political, and diplomatic levers, to achieve victory both in conventional conflict and in the gray zone. The Pentagon must attract and retain service members with the crucial technological skills and scientific competencies that the current system has difficulty engaging. The Pentagon must further ensure that the military and its leadership reflect the diversity of the United States. Building a successful future force with an essential skillset will require the Pentagon to expand its recruiting practices to attract people from diverse backgrounds and experiences.

<sup>171</sup> Tim Kane, *Why Our Best Officers Are Leaving*, The Atlantic (Jan./Feb. 2011) (online at <https://www.theatlantic.com/magazine/archive/2011/01/why-our-best-officers-are-leaving/308346/>).

<sup>172</sup> David Barno and Nora Bensahel, *Can the U.S. Military Halt Its Brain Drain?*, The Atlantic (Nov. 5, 2015) (online at <https://www.theatlantic.com/politics/archive/2015/11/us-military-tries-halt-brain-drain/413965/>).

## National Security Civilian Workforce

A strong civilian national security workforce is an equally critical component of the United States' strategic and military advantage. Like the military, it will need to update its personnel system to attract and retain a diverse group of workers with the critical skills necessary to remain competitive in evolving defense apparatuses. The current antiquated, rigid, and slow-moving personnel system makes it difficult to hire people with the skills its needs, remove workers who are not performing, and promote people who can make the largest contribution.<sup>173</sup>

The lengthy civilian hiring process, which includes extended time for a security clearance background check, drives away talented workers who are unable or unwilling to wait. Programs designed to quickly hire qualified applicants with specialized skills are limited and often not understood by hiring authorities or applicants, and thus hinder efforts to bring in critical talent in STEM, cyber, computer engineering, and other fields.<sup>174</sup>

There are too few incentives for high achievers with specialized in-demand skills and often little accountability for poor performance, which can drive away top talent. Likewise, modern benefits like telework and hours flexibility are limited in the national security community, and there is insufficient opportunity for professional development and educational opportunities. Hiring and pay freezes, government shutdowns, and repeated proclamations that the force is lazy, unnecessary, or unpatriotic harm the morale of the civilian personnel force and make it more difficult for it to recruit and retain talent.

These factors remain significant barriers to recruiting and retaining talent. Also challenging is that notion that the STEM skills required to bolster the national security workforce are also in high demand in the private sector, which usually pays better.

## National Service

Growing a civic-minded and engaged electorate, one that adheres to the premise that informed citizens must participate in democracy for it to function and thrive, is essential to sustaining the American republic and upholding its constitutional mandate to provide for the common defense. The concept of national service builds upon these tenets with a call to action in the vein of AmeriCorps, the Peace Corps, and Teach for America, among others, while providing diverse citizens a shared opportunity to serve their country and communities.

The Brookings Institution argues in a recent report that America's civic health is failing and that increased national service would significantly remedy its decline.<sup>175</sup> This is occurring as

<sup>173</sup> Peter Levine, *Civilian Personnel Reform at the Department of Defense: Lesson from the Failure of the National Security Personnel System*, Institute for Defense Analysis (Oct. 2017) (online at <https://www.ida.org/-/media/feature/publications/c/ci/civilian-personnel-reform-at-the-department-of-defense-lessons-from-the-failure-of-the-national-security-personnel-system/p-8656.ashx>).

<sup>174</sup> Loren DeJonge Schulman, *Managing the National Security Workforce Crisis*, Center for New American Security (May 2019) (online at <https://www.cnas.org/publications/commentary/managing-the-national-security-workforce-crisis>).

<sup>175</sup> John Bridgeland and John DiIulio, *Will America Embrace National Service?*, Brookings Institution (online at [https://www.brookings.edu/wp-content/uploads/2019/10/National-Service\\_TEXT-3.pdf](https://www.brookings.edu/wp-content/uploads/2019/10/National-Service_TEXT-3.pdf)).

adversaries attempt to weaponize American political and societal divisions to weaken the nation. While the idea of compulsory national service is unpopular, there is widespread support<sup>176</sup> for the expansion of voluntary programs, especially in the wake of the COVID-19 pandemic.<sup>177</sup>

In its March 2020 report to Congress “Inspired to Serve,” the National Commission on Military, National, and Public Service identified key shortfalls in civic education and cited the sobering statistic that 22 percent of American adults cannot name any of the three branches of government.<sup>178</sup> The report offers a comprehensive roadmap for increasing citizen engagement and states that “By igniting the extraordinary potential for service, this new approach will address critical national security and domestic needs of the Nation, expand economic and educational opportunities, strengthen the civic fabric of the Nation, and establish a robust culture of service characterized by an expectation that all Americans participate in service of some kind, at some point in their lifetime.”<sup>179</sup>

The case for increased national service is underpinned by the notion that engaging in public service for the common good increases civic capacity and builds social cohesion through shared sacrifice.<sup>180</sup> Developing science, technology, and military national service programs could bolster both the defense apparatus and civil society by enabling collective solutions to public challenges.

<sup>176</sup> Target Point, *Republicans and Democrats Overwhelmingly Support National Service* (online at <http://voicesforservice.org/wp-content/uploads/2015/10/Voices-TP-One-Pager.pdf>).

<sup>177</sup> David Brooks, *We Need National Service. Now.*, The New York Times (May 7, 2020) (online at <https://www.nytimes.com/2020/05/07/opinion/national-service-amicorps-coronavirus.html>).

<sup>178</sup> National Commission on Military, National and Public Service, *Final Report: Inspired to Serve* (Mar. 2020) (online at <https://inspire2serve.gov/sites/default/files/final-report/Final%20Report.pdf>).

<sup>179</sup> *Id.*

<sup>180</sup> David Brooks, *We Need National Service. Now.*, The New York Times (May 7, 2020) (online at <https://www.nytimes.com/2020/05/07/opinion/national-service-amicorps-coronavirus.html>).

## FINANCIAL TRADE-OFFS AND ACQUISITION REFORM

U.S. federal budgets are expected to contract in the near term, even as national security threats become increasingly complex and powerful. Simultaneously, critical domestic needs will compete with defense spending for limited resources. As this tension unfolds, the United States faces a dynamic array of challenges, many of which cannot be solved through traditional defense spending. This new paradigm will require a broad view of what investments are considered critical to the nation's security, as well as hard choices about how to apportion increasingly limited resources.

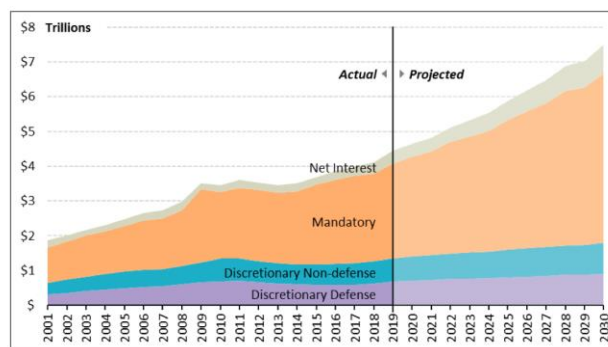
Policy makers, industry, and the Pentagon must work together to identify trade-offs within the defense apparatus to include legacy systems and operations, which will allow for investment in technology and operational concepts to address future challenges. The Pentagon will further need to refine its acquisition process and improve its ability to incorporate innovative emerging technologies and capabilities at the scale required to succeed in an era of great power competition.

### Competing Budget Priorities

In the near term, the United States will likely face contracting federal discretionary budgets (the portion of the federal budget that includes defense), particularly given the enormous cost of confronting the economic and health challenges presented by the COVID-19 pandemic and will need to make difficult decisions about the size of the federal budget and the amount spent on traditional defense investment.

In 2020, the federal budget was more than \$4 trillion, and by 2030 it is expected to be upwards of \$7 trillion. Defense spending, however, is projected to be a more limited percentage of overall federal budgets due to mandatory spending for social programs and interest on the national debt.

**Outlays by Budget Enforcement Category, FY2001–FY2030 (Projected)<sup>181</sup>**  
(in trillions of dollars)



<sup>181</sup> Congressional Research Service, *FY2020 Defense Budget Request: An Overview* (Feb. 20, 2020) (online at <https://crsreports.congress.gov/product/pdf/IN/IN11224>).

The defense budget has historically grown annually in real dollars; however, total defense spending as a share of overall spending, as well as gross domestic product (GDP), has steadily declined since the 1960s.<sup>182</sup> Yet, according to a recent strategic review, the Pentagon anticipates that while real budgetary growth will be flat, the military will require a 3 to 5 percent annual budget increase to implement the National Defense Strategy (NDS) and prepare for great power competition.<sup>183</sup> Conversely, others argue that increased defense spending would make the military less effective by allowing it to avoid making hard choices and permitting it to invest in outdated systems without rethinking how it addresses emerging challenges.<sup>184</sup>

This will occur as pressing domestic needs compete with defense spending as the nation confronts rising income inequality, aging infrastructure, public health and environmental challenges, and other requirements that impact the prosperity and strength of the United States. Addressing these challenges will assure that a strong foreign policy and national defense starts with the homeland.<sup>185</sup>

## The United States and Competitor Countries

With its global obligations and missions, the United States outspends all its rivals combined in defense expenditures. In 2019, it spent more than \$730 billion, while China and Russia spent roughly \$260 billion and \$65 billion, respectively.<sup>186</sup> This is nearly three times as much as China and ten times as much as any other country. While the United States maintains a global military presence and supports a variety of missions, partners, and allies, China and Russia have historically focused on their respective regions, although both are rapidly working to expand their global reach.

China's economy will likely exceed the United States' in dollar terms in the next 10 years.<sup>187</sup> This is a new reality, as the modern United States has never had to compete globally with an economic peer like China. Even during the Cold War, the Soviet Union's economy never equated to more than 57 percent of the U.S. economy.<sup>188</sup> Still, China will face its own challenges as its pace of economic growth appears to slow and it confronts challenges at home such as rising unemployment

<sup>182</sup> *Id.*

<sup>183</sup> Paul McLeary, *Flatline: SecDef Esper Says DoD Budgets Must Grow 3-5%* (Feb. 6, 2020) (online at <https://breakingdefense.com/2020/02/flatline-secdef-esper-says-dod-budgets-must-grow-3-5/>).

<sup>184</sup> Dan Grazier, *How Bells, Whistles & Greed Blew Up the Defense Budget*, Project on Government Oversight (Aug. 4, 2020) (online at <https://www.pogo.org/analysis/2020/08/how-bells-whistles-greed-blew-up-the-defense-budget/>).

<sup>185</sup> William Burns, *The United States Needs a New Foreign Policy*, Defense One (Jul. 15, 2020) (online at <https://www.defenseone.com/voices/william-j-burns/15226/>).

<sup>186</sup> Dave Lawler, *By the Numbers: Military Spending Around the World*, Axios (Apr. 27, 2020) (online at <https://www.axios.com/defense-spending-by-country-us-china-russia-ddbcdba1-6926-434a-87d4-a8794318f3a6.html>).

<sup>187</sup> Michael Brown, Eric Chewning and Pavneet Singh, *Preparing the United States for the Superpower Marathon with China*, Brookings Institution (Apr. 2020) (online at <https://www.brookings.edu/research/preparing-the-united-states-for-the-superpower-marathon-with-china/>).

<sup>188</sup> *Id.*

and managing the expectations of its citizens who increasingly expect consistent improvement in their quality of life.<sup>189</sup>

Regardless, as competitors work to challenge the United States in multiple arenas, the traditional bright lines between defense and non-defense spending will blur, making it essential that the country implements a comprehensive, whole-of-government strategy.

## **Broad View of National Security**

Competitors are using their full range of capabilities, both military and non-military, to confront the United States. To meet these challenges, the United States must invest in whole-of-government tools like diplomacy, foreign economic aid, research and development (R&D), and education.<sup>190</sup>

Former Secretary of Defense Robert Gates argues that U.S. foreign policy has been overmilitarized and that a more robust and empowered State Department should be the cornerstone of the United States' national security strategy, along with more foreign aid, economic tools, and a national strategic messaging plan.<sup>191</sup>

To illustrate a misalignment of priorities, Gates points out that the Pentagon has more military band musicians than the State Department has foreign service officers.<sup>192</sup> Put more bluntly, former Secretary of Defense James Mattis advocated for keeping the State Department and diplomacy at the forefront of American foreign policy by remarking that without a strong State Department, he would need more ammunition for the military.<sup>193</sup>

The Task Force agrees that while a strong military is critical to deter conflict, much of the competition with countries like China will be won in the non-military and information arena. However, many of the instruments and tools of power used to compete in this domain, such as a trade policy that protects American workers and a well-funded State Department, have eroded.<sup>194</sup> To reverse this trend, policy makers will need to apportion finite resources between the traditional

<sup>189</sup> Karishma Vaswani, *How Bad are China's Economic Woes?*, BBC News (May 22, 2020) (online at <https://www.bbc.com/news/business-52754782>).

<sup>190</sup> National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Nov. 2018) (online at <https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf>).

<sup>191</sup> Robert Gates, *The Overmilitarization of American Foreign Policy*, Foreign Affairs (Jul./Aug. 2020) (online at <https://www.foreignaffairs.com/articles/united-states/2020-06-02/robert-gates-overmilitarization-american-foreign-policy>).

<sup>192</sup> NPR, *Military Marching Bands: Your Tax Dollars at Work* (Sept. 2010) (online at <https://www.npr.org/sections/therecord/2010/09/29/130212353/military-marching-bands>).

<sup>193</sup> Department of Defense, *Secretary Mattis Remarks on the National Defense Strategy in Conversation with the United States Institute for Peace* (Oct. 30, 2018) (online at <https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1678512/secretary-mattis-remarks-on-the-national-defense-strategy-in-conversation-with/>).

<sup>194</sup> Robert Gates, *The Overmilitarization of American Foreign Policy*, Foreign Affairs (Jul./Aug. 2020) (online at <https://www.foreignaffairs.com/articles/united-states/2020-06-02/robert-gates-overmilitarization-american-foreign-policy>).

defense and non-defense budgets to buttress these critical aspects of the United States' national security.

Absent a comprehensive and well-funded whole of government approach that utilizes diplomatic, military, economic, information, and other tools, the United States stands to lose to competitor nations willing to challenge it beyond the military arena.<sup>195</sup>

## **Prioritizing Military Objectives**

As part of meeting this challenge, the United States must make difficult choices and better identify its military priorities. Policy makers understand that means and focus are finite, and prioritizing a charge or mission is inherently a decision to place less emphasis elsewhere. For example, a unit deployed to the Middle East to support counterterrorism operations cannot also prepare to deter conflict in the Pacific.

Passing a new authorization for the use of military force (AUMF) after nearly 20 years of war would not only allow Congress to reassert its constitutional power and uphold one of its most crucial duties, it would also afford the opportunity to evaluate the United States' current and future military strategies, missions, and objectives and determine whether they are worthy of the investment and sacrifice. This review and potential reset of the nation's military priorities would help ensure that the Pentagon is best-equipped and supported to protect the United States in current and future dynamic threat environments.

Congress needs to reexamine the necessary operational authorities, including the 2001 AUMF, to continue to sustain global counterterrorism operations and prevent the rise of resurgent violent extremist organizations while preparing to deter near-peer competitors. Congress and the Department of Defense (DOD) must also explore the authorities necessary to more effectively compete in gray zone conflict, with special emphasis on irregular warfare, cyberspace, and information operations.

## **Defense Trade-Offs**

Policy makers, industry, and the Pentagon must similarly identify trade-offs within legacy platforms and equipment to allow for investment in the capabilities necessary to remain competitive in the next century. Currently, the United States is underinvesting in modern technologies while overinvesting in legacy systems that lack the lethality and survivability to be effective in the future.<sup>196</sup>

<sup>195</sup> National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Nov. 2018) (online at <https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf>).

<sup>196</sup> House Committee on Armed Services, *Testimony of Michelle Flournoy, Future of Defense Task Force Hearing: Theories of Victory* (Oct. 29, 2019) (online at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110154> <https://www.congress.gov/116/meeting/house/110154/witnesses/HHRG-116-AS00-Wstate-FlournoyM-20191029.pdf>).



In 2030, a staggering 70 percent of the military is expected to still be composed of legacy systems.<sup>197</sup> This is occurring even as the supply of innovation and emerging technologies is increasing exponentially.

In contrast, China and Russia are less constrained by the need to fund and maintain existing systems and are investing in weapons to undermine the United States' traditional high-end advantage.<sup>198</sup> As an example, China is not attempting to build multiple aircraft carriers to match the United States; rather, it is spending a fraction of that cost to develop anti-ship weapons. Likewise, it is investing in long-range anti-aircraft and strike weapons meant to overwhelm an enemy's defenses, and cyber weapons to undermine the United States' technologically sophisticated systems, many of which are vulnerable to cyber intrusion.<sup>199</sup>

To prepare for these challenges and make the necessary trade-offs, policy makers must determine when it will be more effective to stop spending on legacy capabilities and instead invest in new technologies and equipment.<sup>200</sup> In testimony before the Task Force, former Under Secretary of Defense for Policy Michèle Flournoy framed the debate by asking whether, for example, it might be ultimately more effective to shift funding from a single aircraft carrier and instead use multiple unmanned aerial vehicles (UAVs) for intelligence and surveillance, increase refueling and electronic warfare capability, and utilize long-range strike weapons.<sup>201</sup>

Expanding critical investments in innovative technology and programs will require an increased tolerance for calculated risk at the Pentagon and in Congress. It also requires the discipline to invest in systems and operational concepts necessary to succeed and the will to eliminate those that do not. Correctly navigating these difficult trade-offs will determine whether the United States is able to remain in overmatch against great power competitors.

## The Pentagon Acquisition Process

To meet these challenges and fully incorporate the critical emerging technologies it needs, the Pentagon must make its acquisition process more agile, creative, and less risk-averse. The current system is predisposed and incentivized to invest in incrementally better versions of existing legacy systems, when instead it should be empowered to incorporate new technology that will underpin innovative operational concepts.

<sup>197</sup> Michele Flournoy and Gabrielle Chefitz, *Sharpening the U.S. Military's Edge: Critical Steps for the Next Administration*, Center for a New American Security (Jul. 13, 2020) (online at <https://www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration>).

<sup>198</sup> Chris Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (Apr. 2020).

<sup>199</sup> U.S. Government Accountability Office, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities* (Oct. 2018) (online at <https://www.gao.gov/products/GAO-19-128>).

<sup>200</sup> House Committee on Armed Services, *Testimony of Michelle Flournoy, Future of Defense Task Force Hearing: Theories of Victory* (Oct. 29, 2019) (online at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110154> <https://www.congress.gov/116/meeting/house/110154/witnesses/HHRG-116-AS00-Wstate-FlournoyM-20191029.pdf>).

<sup>201</sup> *Id.*

According to author Chris Brose, who appeared before the Task Force, the Pentagon acquisition process has been optimized for risk aversion and cost accounting, not rapid technology development at scale. This has contributed to a “failure of imagination about America’s rapidly diminishing military dominance.” Brose also notes that the Pentagon often has the legal authority to more quickly integrate new technologies but prioritizes other investments.<sup>202</sup>

The Pentagon must work with Congress to identify needs and innovative capabilities and then ensure that the acquisition process is set up to make substantial investments to procure them at the necessary scale. These types of programs that support new operational concepts should be fast tracked to avoid the “valley of death,” where, too often, initiatives falter and fail to become funded programs of record.

Organizations like the Defense Innovation Unit (DIU) and the Army Future’s Command have addressed these issues and worked to bridge the innovation gap; however, their efforts represent less than 2 percent of the Pentagon’s procurement budget, which is insufficient to deal with emerging challenges or influence innovative companies and investors to pursue partnerships with the DOD.<sup>203</sup> In testimony before the Task Force, former Managing Partner of the DIU Raj Shah suggested that funding for these types of innovation efforts should be increased ten-fold.<sup>204</sup> He further noted that the DOD spends less than \$500 million annually with venture-backed start-ups, which is insufficient to incorporate emerging technologies at scale.

The Pentagon must streamline its cumbersome acquisition process to make it more accessible to smaller and innovative companies. It should further invest in training and incentivizing its acquisition workforce to move more rapidly and take risks when appropriate.<sup>205</sup> Similarly, the DOD should work to adapt its requirement process to be less rigid and sequential and more iterative, which is how software-driven emerging technologies such as artificial intelligence (AI) and autonomous vehicles are developed.<sup>206</sup>

But perhaps most importantly, the nation must fundamentally commit to investing in new technologies and innovative ways of thinking necessary to maintain the military’s advantage as competitor countries work to develop and implement their own breakthrough capabilities. And, as

<sup>202</sup> Chris Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (Apr. 2020).

<sup>203</sup> Michael Brown, Eric Chewning, and Pavneet Singh, *Preparing the United States for the Superpower Marathon with China*, Brookings Institution (Apr. 2020) (online at <https://www.brookings.edu/research/preparing-the-united-states-for-the-superpower-marathon-with-china/>).

<sup>204</sup> House Committee on Armed Services, *Testimony of Raj Shah, Future of Defense Task Force Hearing: Supercharging the Innovation Base* (Feb. 5, 2020) (online at <https://armedservices.house.gov/2020/2/future-of-defense-task-force-hearing-supercharging-the-innovation-base>).

<sup>205</sup> *Id.*

<sup>206</sup> Michele Flournoy and Gabrielle Chefetz, *Sharpening the U.S. Military’s Edge: Critical Steps for the Next Administration*, Center for a New American Security (Jul. 13, 2020) (online at <https://www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration>).

noted in testimony before the Task Force by former Secretary of the Army Eric Fanning, the formation of Space Force provides an auspicious opportunity to implement these reforms.<sup>207</sup>

<sup>207</sup> House Committee on Armed Services, *Testimony of Eric Fanning, Future of Defense Task Force Hearing: Supercharging the Innovation Base* (Feb. 5, 2020) (online at <https://armedservices.house.gov/2020/2/future-of-defense-task-force-hearing-supercharging-the-innovation-base>).



## OPERATIONAL CONCEPTS

The Pentagon must hone its operational concepts to address the 21<sup>st</sup>-century challenges posed by Russia, China, and other emerging threat streams. Even while it remains an economic heavyweight, America can no longer edge out its competition solely by outspending potential foes. It must employ and focus its military more effectively to defend its forward bases, sustain its forces, protect its information and communication systems, defend against long-range strike capabilities, and deter and defeat strategic weapons. Likewise, new strategies must effectively dissuade competitors from challenging the United States in the gray zone of hybrid warfare with weapons like information warfare, economic coercion, and attacks on democracy and elections.

In testimony before the Task Force, former Under Secretary of Defense for Policy Michèle Flournoy stated that Russia and China will likely achieve military overmatch in a number of areas, challenging the United States' ability to deter aggression and prevail in future conflicts.<sup>208</sup> Likewise, then Chairman of the Joint Chiefs General Joseph Dunford told Congress that the United States was on track to lose its qualitative and quantitative military advantage without changing trajectory.<sup>209</sup> And a sobering report from the RAND Corporation recently found that despite significantly outspending China and Russia, the U.S. military could lose future conflicts because it failed to adequately posture to defeat modernizing adversaries.<sup>210</sup>

### The Need for Updated Operational Concepts

The Pentagon must adapt its operational concepts to effectively utilize and posture its military capabilities to address significant challenges posed by strategic competitors like China and Russia. The National Defense Strategy (NDS) recognizes the need to adjust: "We must anticipate how competitors and adversaries will employ new operational concepts and technologies to attempt to defeat us, while developing operational concepts to sharpen our competitive advantages and enhance our lethality."<sup>211</sup> Accurately predicting future conflicts is challenging in any era, and many of the Pentagon's current operational concepts and associated structures were established in the wake of the Cold War, when the United States enjoyed decisive military superiority.

<sup>208</sup> House Committee on Armed Services, *Testimony of Michelle Flournoy, Future of Defense Task Force Hearing: Theories of Victory* (Oct. 29, 2019) (online at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110154> <https://www.congress.gov/116/meeting/house/110154/witnesses/HHRG-116-AS00-Wstate-FlournoyM-20191029.pdf>).

<sup>209</sup> Senate Committee on Armed Services, *Testimony of General Joseph Dunford, Hearing on Department of Defense Budget Posture* (Jun. 13, 2017) (online at <https://www.armed-services.senate.gov/hearings/17-06-13-department-of-defense-budget-posture>).

<sup>210</sup> David Ochmanek, Peter Wilson, Brenna Allen, John Speed Meyers, and Carter Price, *U.S. Military Capabilities and Forces for a Dangerous World*, RAND Corporation (2017) (online at [https://www.rand.org/pubs/research\\_reports/RR1782-1.html](https://www.rand.org/pubs/research_reports/RR1782-1.html)).

<sup>211</sup> Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Strengthening American Military's Competitive Advantage* (2018) (online at <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>).

Then, the battlefield was primarily limited to the domains of air, land, and sea, and rogue nations with limited military capacity were the greatest emerging threats. Unlike today, there were no strategic competitors. Now, in both conventional warfare and gray zone tactics, Russia and China are able to challenge the United States in multiple arenas.<sup>212</sup> Indeed, it is what they have been preparing for over the last two decades while the United States was focused on countering terrorism.

Both China and Russia have integrated asymmetric approaches and technologies that present significant military challenges in the event of overt conflict with the United States, most notably by advancing anti-access/area denial (A2/D2) capabilities. China is prioritizing the development of so-called Assassin's Mace weapons, inexpensive platforms like anti-satellite weapons, anti-aircraft carrier missiles, and radar jammers designed to exploit the vulnerabilities of ostensibly superior militaries.<sup>213</sup> As the story of David and Goliath illustrates, a seemingly stronger force can be defeated by a less capable opponent that can deftly deploy its strengths against a slower-adapting adversary.

Associated operational concepts that countries like Russia and China are developing are designed to achieve this advantage. As an example, part of China's military doctrine increasingly relies on "system destruction" warfare, which takes down an opponent's networks and cripples the flow of information while degrading national resolve. Likewise, a large part of Russia's strategy is the pursuit of a more modern and robust nuclear arsenal to support its "escalate to deescalate" doctrine.<sup>214</sup> Alongside China and Russia, countries such as Iran and North Korea are honing similar capabilities that will likely allow them to challenge the U.S. military in unprecedented ways in the event of conventional military conflict.

Many U.S. defense officials assert that great power competition, including with China and Russia, will continue to occur below the threshold of major conflict in the gray zone, calculated to circumvent the United States' traditional hard power military advantage.<sup>215</sup> These actors will continue to employ weaponized misinformation, proxy forces, espionage, economic coercion, and cyber and electronic attacks to challenge the United States and its allies.

## Effective Operational Concepts

The U.S. military services are developing new offensive and defensive operational concepts to maintain an advantage while also serving as a credible deterrent. A recent analysis from the RAND Corporation found that the chance of conflict with China and Russia will likely rise as their military capability relative to the United States' increases and the balance of military power continues

<sup>212</sup> *Id.*

<sup>213</sup> Don Tse, *China's Americanized Military*, *The Diplomat* (Dec. 13, 2017) (online at <https://thediplomat.com/2017/12/chinas-americanized-military/>).

<sup>214</sup> House Committee on Armed Services, *Testimony of Michelle Flournoy, Future of Defense Task Force Hearing: Theories of Victory* (Oct. 29, 2019) (online at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110154> <https://www.congress.gov/116/meeting/house/110154/witnesses/HHRG-116-AS00-Wstate-FlournoyM-20191029.pdf>).

<sup>215</sup> Lyle Marris et al., *Gaining Competitive Advantage in the Gray Zone*, RAND Corporation (Jun. 2019) (online at [https://www.rand.org/pubs/research\\_reports/RR2942.html](https://www.rand.org/pubs/research_reports/RR2942.html)).

to shift away from the United States.<sup>216</sup> To reverse this trend, the Pentagon is developing and refining multiple new operational concepts.

The Army and Air Force are working jointly on operations, which incorporate capability across multi-domains to maintain superiority. Similarly, the Air Force is pursuing future operating concepts and agile combat employment to disperse increasingly networked forces away from large bases to make them more effective and survivable in a contested environment.<sup>217</sup>

The Navy and Marines are developing maritime operations to make naval forces more distributed and networked. This is in addition to the expeditionary advanced base operations of the Marine Corps, which set up a forward presence at sea and enable long-range strike capability.<sup>218</sup> And notably, the Marines Corps has proposed significant reforms to the way it trains, operates, and equips with its Force Design 2030 report, including significant trade-offs in focus and investment.<sup>219</sup>

These initiatives integrate capabilities and information across domains and disperse forces so they are less concentrated and vulnerable to attack. They integrate and network the military, enabling it to utilize more unmanned systems and incorporate newly emerging technologies.<sup>220</sup>

For this reason, doctrinal and technological innovations like DARPA's "Mosaic Warfare," a concept designed to send a variety of networked weapons and small sensor platforms to overwhelm an enemy, will be central. The concept envisions a scenario where ubiquitous and affordable unmanned air and ground platforms find targets on a contested battlefield and pass the information to a decision maker who can instantly task another part of the same system to strike the enemy from safety.<sup>221</sup> This follows a similar DARPA initiative, Assault Breaker II, designed to counter a competitors' ability to use its A2/D2 capability to gain control of critical territory. Assault Breaker II coordinates a nearly immediate response strike against critical enemy sites and nodes without risking larger-scale escalation, which would require the ability to find targets using long-range sensors networked to strike capabilities.<sup>222</sup>

Initiatives like these illustrate that victory on the battlefield of the future will be less about the capability and quality of individual weapons and more about the sum of many systems working

<sup>216</sup> Raphael Cohen et al., *The Future of Warfare in 2030*, RAND Corporation (May 2020) (online at [https://www.rand.org/pubs/research\\_reports/RR2849z1.html](https://www.rand.org/pubs/research_reports/RR2849z1.html)).

<sup>217</sup> Valerie Insinna, *The US Air Force has unconventional plans to win a war in the Asia-Pacific*, Defense News (Feb. 10, 2020) (online at <https://www.defensenews.com/digital-show-dailies/singapore-airshow/2020/02/11/the-us-air-force-has-unconventional-plans-to-win-a-war-in-the-asia-pacific/>).

<sup>218</sup> Jake Yaeger, *Expeditionary Advanced Maritime Operations: How the Marine Corps Can Avoid Becoming a Second Land Army in the Pacific*, War on the Rocks (Dec. 26, 2019) (online at <https://warontherocks.com/2019/12/expeditionary-advanced-maritime-operations-how-the-marine-corps-can-avoid-becoming-a-second-land-army-in-the-pacific/>).

<sup>219</sup> Department of the Navy, *Force Design 2030* (Mar. 2020) (online at <https://www.hqmc.marines.mil/Portals/142/Docs/CMC38%20Force%20Design%202030%20Report%20Phase%20I%20and%20II.pdf?ver=2020-03-26-121328-460>).

<sup>220</sup> Congressional Research Service, *Renewed Great Power Competition Implication for Defense—Issues for Congress* (Aug. 25, 2020) (online at <https://fas.org/sgp/crs/natsec/R43838.pdf>).

<sup>221</sup> Defense Advanced Research Projects Agency, *DARPA Tiles Together a Vision of Mosaic Warfare* (Sept. 2020) (online at <https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosaic-warfare>).

<sup>222</sup> Department of Defense, *2017 Summer Study on Long Range Effects*, Defense Science Board (2017) (online at [https://dsb.cto.mil/reports/2010s/LRE%20Executive%20Summary\\_\\_Final.pdf](https://dsb.cto.mil/reports/2010s/LRE%20Executive%20Summary__Final.pdf)).

together. This will make seamless joint command and control, training, and doctrine critical. So, too, will be common technology, communication, and interoperability, particularly as artificial intelligence-enabled technology rapidly increases the speed of conflict and decision making on the battlefield.

This concept of “algorithmic warfare” will pit algorithms against algorithms where information and the speed of decisions will likely be more important than traditional means of military superiority, such as the size of opposing forces or the range of armament. Those with superior data, computing power, information security, and connectivity will maintain the upper hand. This paradigm will require new operational concepts and equipment to adapt and maintain the advantage.<sup>223</sup>

Military partnerships and alliances will be force multipliers for the United States in both large-scale and gray zone conflict. A recent report from U.S. Indo Pacific Command on how to maintain the United States military’s supremacy places a high priority on strengthening allies and partners, as well as their interoperability and coordination with U.S. forces.<sup>224</sup> In fact, many of the Pentagon’s new operational concepts are wholly dependent on allies to allow for the wide distribution of U.S. forces and bases.<sup>225</sup>

While the military has been aggressively working to address emerging challenges and leverage new, innovative technology, many emerging operational concepts are not yet fully validated and supported with the necessary capabilities, investments, and technologies.

## Review of Nascent Operational Concepts

The Pentagon must continue to develop effective operational concepts to address emerging challenges while directly correlating them with investments and programs of record. While the military has taken significant steps to modernize and prepare for the future, it is not yet fully organized and equipped to confront emerging threats and take advantage of new opportunities; it remains predisposed to capabilities and institutions developed in the 20<sup>th</sup> century.<sup>226</sup>

A recent nonpartisan review of the 2018 NDS commissioned by Congress affirmed that the Pentagon has had difficulty developing new, fully workable operational concepts, notably to counter China and Russia in both the gray zone and conventional conflict.<sup>227</sup> According to the review, “detailed, rigorous operational concepts for solving these problems and defending U.S. interests are

<sup>223</sup> National Security Commission on Artificial Intelligence, *Interim Report* (Nov. 2019) (online at <https://drive.google.com/file/d/153OrxnuGEjsUvIxWsFYauslwNeCEkvUb/view>).

<sup>224</sup> U.S. Indo-Pacific Command, *NDAA 2020 Section 1253 Assessment Executive Summary* (Sept. 2020) (online at <https://int.nyt.com/data/documenthelper/6864-national-defense-strategy-summ/8851517f5e10106bc3b1/optimized/full.pdf>).

<sup>225</sup> Miranda Priebe, Alan Vick, Jacob Heim, and Meagan Smith, *Distributed Operations in a Contested Environment*, RAND Corporation (2019) (online at [https://www.rand.org/pubs/research\\_reports/RR2959.html](https://www.rand.org/pubs/research_reports/RR2959.html)).

<sup>226</sup> Richard Danzg et al., *A Preface to Strategy: The Foundation of American National Security*, Johns Hopkins Advanced Physics Lab (May 2018) (online at <https://www.jhuapl.edu/Content/documents/PrefaceToStrategy.pdf>).

<sup>227</sup> National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Nov. 2018) (online at <https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf>).



badly needed, but do not appear to exist.” Although the Pentagon has laudably refined its vision for the force of the future, it has yet to fully organize, procure, and deploy the capability to fully translate this vision into workable operational concepts.<sup>228</sup>

Author Chris Brose, who testified before the Task Force, discusses in his recent book *The Kill Chain* how, in wargames simulating conflict with China in the Eastern Hemisphere over the last decade, the United States lost nearly every time.<sup>229</sup> In such scenarios, much of the needed military capability was thousands of miles away and would come under persistent attack while attempting to reach the battlefield. Cyber-attacks would frustrate logistics and communications and critical satellites used for intelligence, and global positioning systems would likely be degraded. American bases and forces in the Pacific would come under sustained attack from long-range precision munitions with insufficient defenses.<sup>230</sup>

This scenario plays out, in part, because the military’s investment in modern platforms has not sufficiently matched its ability to protect its forces and integrate them into new operational concepts. For example, high-end platforms like the F-35 are of little value if the military cannot protect and supply the bases from which they need to operate. The Pentagon has prioritized the purchase of these types of high-end systems without sufficiently balancing the need to procure associated enabling capabilities such as defending forward bases, ensuring supply chain logistics for fuel and munitions, and securing networking and communications.<sup>231</sup>

The military is developing game-changing operational concepts to take advantage of new innovative technology and thinking but has yet to fully procure the systems and capacity to fully implement initiatives like Mosaic Warfare and Assault Breaker II. For these reasons, the Pentagon must enhance its capability, expertise, and processes to rigorously define military challenges, and it must design and correlate programs of record to address and incorporate them into new operational concepts.

To that end, the military must work with Congress to more directly connect its investments with its key priorities in support of operational concepts. It should engage a diverse group of stakeholders, including Congress, academia, think tanks, and the private sector, to develop imaginative solutions to emerging problems and help assess the Pentagon’s efforts.<sup>232</sup> It will also be essential to test, experiment, and wargame new operational concepts as well as prototype and test the technology that underpins them, such as networked unmanned systems. Creative concepts and

<sup>228</sup> House Committee on Armed Services, *Testimony of Michelle Flournoy, Future of Defense Task Force Hearing: Theories of Victory* (Oct. 29, 2019) (online at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110154> <https://www.congress.gov/116/meeting/house/110154/witnesses/HHRG-116-AS00-Wstate-FlournoyM-20191029.pdf>).

<sup>229</sup> Chris Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (Apr. 2020).

<sup>230</sup> *Id.*

<sup>231</sup> Sen. Jim Inhofe and Sen. Jack Reed, *The Pacific Deterrence Initiative: Peace Through Strength in the Indo-Pacific*, War on the Rocks (May 28, 2020) (online at <https://warontherocks.com/2020/05/the-pacific-deterrence-initiative-peace-through-strength-in-the-indo-pacific/>).

<sup>232</sup> National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Nov. 2018) (online at <https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf>).

development wargaming can also provide guidance on how to use legacy platforms and capability to address deficiencies—essentially using existing technology in creative ways to address emerging problems.<sup>233</sup>

The most effective military operational concepts and associated military capacity, however, will still be insufficient in addressing the breadth of the challenges posed by strategic competitors. A whole-of-nation effort, including military tools, trade policy, STEM education, diplomatic initiatives, and further non-military instruments, is necessary to meet these emerging threats. Without this approach, the United States will not be postured to maintain its security and global influence, even if the military is robustly equipped and funded. The problems competitors present are comprehensive, and the nation's response must be equally broad.<sup>234</sup>

<sup>233</sup> House Committee on Armed Services, *Testimony of Michelle Flournoy, Future of Defense Task Force Hearing: Theories of Victory* (Oct. 29, 2019) (online at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110154><https://www.congress.gov/116/meeting/house/110154/witnesses/HHRG-116-AS00-Wstate-FlournoyM-20191029.pdf>).

<sup>234</sup> National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Nov. 2018) (online at <https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf>).

## BRIEFERS

**Rear Adm. Jeffrey T. Anderson, USN**  
Deputy Director for Political-Military Affairs  
(Asia)  
J5, Joint Staff

**Jim Baker**  
Director of the Office of Net Assessment  
Department of Defense

**Dr. Robert Bakos**  
Principal and Co-Founder  
Innoveering

**Scott W. Bray**  
Deputy Director Naval Intelligence and  
Director of the Naval Intelligence Activity  
Deputy Chief of Naval Operations for  
Information Warfare/Director of Naval  
Intelligence

**Michael Brown**  
Director  
Defense Innovation Unit

**Andrew D. Cox**  
Director, Space Security and Defense  
Program  
Air Force Space Command  
Senior Analyst, Nimitz Operational  
Intelligence Center  
Office of Naval Intelligence

**Matthew C. Cummings**  
Deputy Director, Technical Collection Office  
Office of the Under Secretary of Defense for  
Intelligence and Security

**Col. Charles W. Del Pizzo, USMC**  
Division Chief, Oceania, South & Southeast  
Asia, DD-Asia  
Joint Staff

**Dr. Diane DiEuliis**  
Senior Research Fellow  
National Defense University

**Alex Gallo**  
Executive Director  
The Common Mission Project

**Rear Adm. David J. Hahn, USN**  
Chief of Naval Research  
Director of Innovation, Technology  
Requirements and Test & Evaluation

**Dennis R. Helmich**  
Director, Integrated Military Systems  
Sandia National Laboratories

**Lt. Gen. S. Clinton Hinote, USAF**  
Deputy Director  
Air Force Warfighting Integration Capability

**Christopher B. Johnstone**  
Principal Director for South and Southeast  
Asia  
Office of the Secretary of Defense

**Elsa Kania**  
Research Fellow  
Center for Security and Emerging  
Technology,  
Georgetown University

**Dr. Jason Kelly**  
Co-founder and CEO  
Gingko Bioworks

**Dr. Theresa Mayer**  
Executive Vice President of Research  
Purdue University

**Tom Nelson**  
Director, BMNT, Inc.

**David Ochmanek**  
Senior Defense Analyst  
RAND Corporation

**Dr. Joel Predd**  
Director, Acquisition and Technology Policy  
Center  
RAND Corporation

**Dr. Will Roper**  
Assistant Secretary of the Air Force for  
Acquisition, Technology and Logistics

**Lt. Gen. John N.T. Shanahan, USAF**  
Director, Joint Artificial Intelligence Center  
Department of Defense

**Col. Timothy D. West, USAF**  
Deputy Director, Aerospace Systems  
Directorate  
Air Force Research Laboratory

**Amy F. Woolf**  
Nuclear Weapons Policy  
Congressional Research Service  
Library of Congress

## HEARINGS

### **Theories of Victory**

October 29, 2019

#### **Ms. Michèle Flournoy**

Co-founder and Managing Partner  
WestExec Advisors

#### **Senator Jim Talent**

Co-chair  
Reagan Institute Task Force

### **Supercharging the Innovation Base**

February 5, 2020

#### **The Honorable Eric Fanning**

President and CEO  
Aerospace Industries Association

#### **Mr. Raj Shah**

Chairman and Co-founder  
Arceo.ai

#### **Mr. Chris Brose**

Chief Strategy Officer  
Anduril

## CONGRESSIONAL DELEGATIONS

### **Halifax International Security Forum**

November 22, 2019—November 24, 2019  
Halifax, Canada

#### **Asia**

January 17, 2020—January 24, 2020  
Vietnam  
Cambodia  
Thailand

### **Munich Security Conference**

February 14, 2020—February 15, 2020  
Munich, Germany

#### **Africa**

February 16, 2020—February 20, 2020  
AFRICOM  
Djibouti  
Kenya

### **Silicon Valley and Boston**

February 17, 2020—February 21, 2020  
San Francisco, Palo Alto, Menlo  
Park, Mountain View & San  
Mateo, California, US  
Boston & Cambridge,  
Massachusetts, US

## ACKNOWLEDGEMENTS

The Co-Chairs of the Future of Defense Task Force would like to thank the following people and organizations for their support:

**Graham Allison**

Douglas Dillon Professor of Government  
Harvard Kennedy School

**Ash Carter**

Former Secretary of Defense

**James Cross**

Founder  
Silicon Valley Defense Working Group

**The Honorable Ron Estes**

Member of Congress  
(R-Kan.)

**Dr. Kathleen Hicks**

Senior Vice President  
Center for Strategic & International Studies

**Col. William F. McCollough, USMC**

Director, House Legislative Affairs

**Lt. Cameron McCord, USN**

House Legislative Affairs

**David Petraeus**

Former Director  
Central Intelligence Agency

**Maj. Jonathan E. Pettibon, USMC**

Deputy Director, House Legislative Affairs

**The Reagan Institute**

**The Honorable Adam Smith**

Chairman, House Armed Services Committee  
(D-Wash.)

**The Honorable William “Mac”**

**Thornberry**

Ranking Member, House Armed Services  
Committee  
(R-Texas)

**Col. Wayne Turnbull**

Defense Attaché to Thailand  
U.S. Army

**Robert O. Work**

Former Deputy Secretary of Defense

The Co-Chairs would like to recognize their families for their support and sacrifice:

Congressman Moulton would like to thank his wife Liz, and their daughter, Emmy.

Congressman Banks would like to thank his wife Amanda, and their three daughters.

The Co-Chairs would also like to thank the following staff:

**Christine Wagner**  
Legislative Director  
Office of Congressman Seth Moulton

**Lindsay Ratliff**  
Legislative Director  
Office of Congressman Jim Banks

**Laura Rauch**  
Senior Investigator  
House Armed Services Committee

**Troy Nienberg**  
Counsel  
House Armed Services Committee

**Eric Snelgrove**  
Professional Staff Member  
House Armed Services Committee

**Emma Morrison**  
Clerk  
House Armed Services Committee

**Natalie de Benedetti**  
Clerk  
House Armed Services Committee

**Rory Coleman**  
Clerk  
House Armed Services Committee