The Institute for Foreign Policy Analysis

National Security Update

Accessing the Technologies and Capabilities of the U.S. Commercial High-Tech Sector: A Defense Department Priority

Our thirteenth *IFPA National Security Update* examines the growing need of the Department of Defense to access and leverage the advanced dual-use technologies increasingly being developed in the commercial high-tech sector to maintain U.S. technological and military superiority. It focuses on the impediments facing the U.S. government and Defense Department in accessing commercial high-tech technologies, strategies and policies to remove these impediments, specific programs and initiatives to address the problem, and the concerns about the growing technological and military capabilities of China.

Topics addressed in our *National Security Update* series include the FY2020 National Defense Authorization Act, hypersonic missiles, military applications of artificial intelligence, missile defense priorities, the Trump Administration's Executive Order on Electromagnetic Pulse, the status of the Space Force, and China's actions in the South China Sea and U.S. options. *IFPA Updates* are posted on our website at www.ifpa.org/.

Key Conclusions and Findings

- The FY 2020 NDAA contains several positive elements and significant contributions to U.S. defense policy and programs. It also has weaknesses and shortcomings.
- Today, most advanced technologies with direct military/defense applications – i.e., dual-use technologies – are developed and produced by the commercial sector. Research and development (R&D) funding in the U.S. (and foreign) commercial sector now far exceeds R&D spending by the Department of Defense (DOD). These two factors have significant implications for how DOD acquires such technologies and its ability to preserve military superiority.
- The U.S. military's technological advantage is eroding because these advanced, dual-use technologies are becoming more widely available on a global basis. Although some progress has been made, DOD has been slow to leverage the advanced dual-use technologies developed in the commercial sector such as artificial intelligence, cloud computing, quantum computing, autonomy, robotics, 3D printing, the Internet of Things, and advanced wireless technologies/networks/5G. This trend is accelerating.
- Its growing capabilities and strategy to achieve global technological dominance make China our leading competitor. Unlike in the United States, few political, legal, economic, or cultural roadblocks exist in China to prevent collaboration across such sectors as industry, academia, research labs, the military, and government. This allows the Chinese government to control technology development priorities and funding.

- The U.S. government, DOD, Congress, and traditional defense industry suppliers need to develop strategies, enact policies, make organizational changes, shed long-held cultural biases and outdated business practices, and encourage non-traditional high-tech commercial firms to work with DOD. DOD needs to develop a more integrated acquisition structure to include closer collaboration and partnership with the government defense/national security enterprise, with the commercial sector, traditional defense suppliers, and academia.
    - These efforts are essential if the U.S. defense enterprise is to benefit more fully from leading-edge commercial technologies.
- As the Trump Administration's National Security Strategy and National Defense Strategy acknowledge, current DOD acquisition processes do not provide timely decisions, policies, and capabilities to the warfighter. Both documents describe the shifting global research and development environment. The United States can best ensure U.S. technological preeminence by:
    - Identifying the various impediments within DOD and the government for accessing commercial-sector technologies and capabilities more effectively;
    - Implementing structural and cultural changes within the Defense Department to support innovation by streamlining the integration of commercial technology across the U.S. defense/national security enterprise; and,
    - Creating strategic partnerships to align private sector R&D resources to priority defense/national security applications.
- In support of these efforts, important specific initiatives have already been undertaken that provide a basis for further action. These include:
    - Changes in the organization of the Pentagon's R&D activities;
    - Creation of new acquisition policies and authorities;
    - Actions to change the DOD acquisition culture and increase the speed of fielding systems;
    - Establishing a presence in key U.S. technology hubs;
    - Establishment of venture capital entities within the government and DOD (e.g., In-Q-Tel, the Defense Innovation Unit, and Army Venture Capital Initiative) and in major defense contractors to identify technologies and encourage commercial startups to work with DOD and the defense industry; and,
    - Use of other transaction authority (OTA) agreements to facilitate the participation of non-traditional defense companies and startups in DOD efforts. OTAs allow speedier contract awards by relaxing/doing away with many of DOD's complicated contracting requirements and stipulations which discourage commercial startups and potential non-traditional suppliers from working with the Defense Department.
- A key challenge facing DOD in gaining greater commercial-sector participation in defense projects is an anti-defense culture in some high-tech firms as evidenced by Google's exit from DOD's Project Maven, a program to use artificial intelligence to help track down

terrorists. This anti-defense bias puts the United States at an inherent disadvantage with countries such as China.

- To rectify this situation and to make pursuing defense opportunities a more enticing and profitable option for commercial companies, several priority efforts should be undertaken including:
    - Mitigating high-tech's anti-defense culture by outreach underscoring that DOD and commercial high-tech companies have shared values in helping to ensure a strong U.S. economy and defense;
    - Incentivizing high-tech companies by easing the onerous DOD contracting regulations and utilizing OTAs more frequently; and,
    - Protecting a company's intellectual property.

Introduction

The National Defense Authorization Act (NDAA) is the annual defense policy bill which, as the name implies, authorizes the Pentagon to undertake various defense-related activities and procurements. The actual money to fund these activities comes from the annual defense appropriation bills, one of which appropriates funds for the Department of Defense and other defense/national security related functions.

Over the past several years, the White House, Department of Defense (DOD) officials, members of Congress, and national security experts have expressed growing concern that the long-held technological edge of the U.S. military is eroding. This erosion is attributed to the increased development of advanced technologies outside the defense sector and the growing availability of these technologies to our adversaries because of globalization. This situation is exacerbated by the entrenched organizational and cultural barriers within DOD that impede incorporating and exploiting commercial innovations.

The Defense Department has not sufficiently tapped into the leading-edge commercial companies and non-traditional suppliers, historically not part of the DOD innovation ecosystem, but which are now the source of the majority of research and development (R&D) spending and where most of the advanced technologies and capabilities needed to sustain U.S. military superiority are being developed. DOD has been slow to assimilate these new technologies/capabilities and turn them into usable warfighting tools. In today's digital age, innovation more frequently comes from smaller entrepreneurs than from the industry structures that were the hallmark of 20th-century government and business.

Among the challenges confronting DOD are adjusting its current organizations and business models and developing new ones to access more effectively the technologies developed in the private sector, changing its business culture to seek out and welcome technologies developed outside of DOD and its traditional contractor base, and discovering more successful approaches to leverage commercial technologies/capabilities for defense applications.

The U.S. government, DOD, and Congress, together with the traditional defense industry suppliers, need to build on existing strategies and policies, to make organizational changes and shed long-held cultural biases and outdated business practices as well as to encourage non-traditional high-tech commercial firms to work with DOD. These continuing efforts are

essential if the U.S. defense enterprise is to incorporate leading-edge commercial technologies more rapidly.

In particular, DOD needs to develop a more integrated acquisition structure to include closer collaboration and partnership with organizations in the government defense/national security enterprise, with the commercial sector, traditional defense suppliers, and academia.

Background: The Changed R&D and Technological Landscape

The technological dominance of the U.S. military has provided a decisively important counter against U.S. adversaries. In the generation after World War II, the U.S. government (USG), and specifically the Department of Defense, was the major driver of the worldwide R&D and technology environment.

To illustrate, the USG in 1960 accounted for 69% of global R&D with U.S. defense R&D representing 36% of that total. However, from 1960 to 2016, the USG's percentage of R&D worldwide dropped to 28% while its share of total U.S. R&D fell from 65% to 24% as R&D conducted by U.S. business doubled from 33% to 67%. As a consequence of these developments, by 2016 U.S. defense R&D dipped to only 3.7% of total global R&D, principally because of an upsurge in both public and private R&D spending by other countries coupled with augmented R&D funding by U.S. companies and USG nondefense R&D.[i]

The effect of this sizable fall-off in defense R&D spending as a segment of worldwide R&D combined with the doubling of business R&D spending was that increasingly many of the most advanced technologies with direct military/defense applications – i.e., dual-use technologies – were now being produced by the commercial sector. This includes most Fourth Industrial Revolution[ii] technologies such as artificial intelligence, cloud computing, quantum computing, autonomy, robotics, 3D printing, the Internet of Things, and advanced wireless technologies/networks/5G. This trend is accelerating.

Because of several factors, the speed and cost of innovation in today's commercial-sector ecosystem is far greater than what the USG and DOD can sustain. This is particularly the case given the wide range of technologies that the Defense Department requires in its weapon systems.

Because of these trends, many defense officials and national security experts have recognized the dramatic changes in the worldwide R&D environment combined with DOD's growing reliance on technologies developed in the private sector for the commercial market. This reality has significant ramifications about how DOD must prepare itself to access needed technologies.

Growing Concerns about China

The decisive military advantage the United States had long held over its adversaries and peer competitors is increasingly fading. Globalization has fueled commercial innovation sparked by research investments that now far surpass DOD R&D spending. In addition, the commercial development of advanced technologies coupled with globalization has allowed both state and non-state actors to gain access to technologies that greatly enhance their offensive capabilities which now enables some to compete in several domains of warfare.

However, China is the most serious U.S. competitor because of its growing technological capabilities, together with its integrated civilian-commercial-military strategy for achieving technological dominance worldwide. China has become a global science and technology leader with its share of global R&D rising from 4.9% in 2000 to 25.1% in 2016.[iii] Beijing is focusing on several dual-use technologies including artificial intelligence (AI), quantum computing, autonomous systems, robotics, nanotechnology, augmented reality/virtual reality, financial technology, and gene editing to name a few.

China has produced several national plans and initiatives outlining its technological and economic goals. Two in particular, *Made in China 2025*, published in 2015, and the 2017 *Next Generation AI Development Plan,*[iv] form the foundation of Beijing's technology strategy. The *Next Generation AI* document is representative of its overall strategy and goals regarding the technologies China has identified as critical for both economic and military power. This document describes a three-step plan for global AI ascendancy in this decade:

1. To keep pace with the leading global AI technologies and applications by 2020;
2. To achieve AI breakthroughs by 2025; and,
3. To be the world leader in artificial intelligence by 2030.[v]

Unlike in the United States, few political, legal, economic, or cultural roadblocks exist in China to prevent collaboration across sectors such as industry, academia, research labs, the military, and government. To illustrate, in 2017 Beijing established the Military-Civil Fusion Development Commission with the goal of accelerating the transfer of AI technology and other advanced technologies from both Chinese commercial firms and academic research institutions to the People's Liberation Army. This unified, near-seamless technology-sharing effort in China allows the government the means to determine technology development priorities and funding.

China seeks to minimize dependence on foreign technology, develop home-grown technological and innovation capabilities, and eliminate the military gap with the United States. As outlined in the *Next Generation AI Development Plan* and *Made in China 2025* documents cited above, China has put in place a multi-pronged strategy to achieve global technology leadership.

China utilizes both legal and illegal means to achieve the goals of this strategy. This includes pilfering foreign, but especially U.S., intellectual property via espionage and cybertheft; foreign direct investment; China-based venture capital focusing on early-stage high-tech firms developing technologies targeted by Beijing, together with investments by Chinese companies in U.S. venture-backed deals (e.g., between 2010 and 2017 Chinese venture capital investments in U.S. AI companies totaled approximately $1.3 billion);[vi] purchase of foreign firms; and sending Chinese students to study science, technology, engineering, and mathematics (STEM) in the United States and other Western nations (approximately 25% of all U.S. STEM graduate students are Chinese nationals) who take back to China Western technological expertise, and in some cases, purloined intellectual property.[vii]

The Trump Administration, Defense Department, and Congress are increasingly alarmed by these Chinese efforts and believe the USG approach to safeguard critical technologies has been ineffective. Several Executive Branch officials and members of Congress have called for tighter

regulation of China's acquisition of foreign companies by giving a broader mandate to the Committee on Foreign Investment in the United States.

President Trump has also banned the sale of U.S. technology to the Chinese tech giant Huawei whose goal is to dominate the global development of the 5G Internet network. Administration officials believe that Huawei is "a Trojan Horse for Beijing's cyberspies"[viii] with "backdoors" built into communication channels as part of Huawei's equipment.

Fearing that the Chinese government will have anytime access to these backdoors, the United States has pressed U.S. allies not to utilize Huawei 5G equipment with some successes. Australia, New Zealand, Japan, and Taiwan have agreed to ban future purchases of Huawei products in their mobile networks and phase out current Huawei equipment.

However, on January 28, 2020 the United Kingdom decided not to bar outright the use of Huawei technology. The United Kingdom will allow Huawei to provide 35% of its 5G network but ban the company from contributing core elements to the network which the British government claims will provide adequate safeguards preventing Chinese spying and espionage. The decision was a setback for the Trump Administration and may adversely impact the U.S.-UK "special relationship."

Canada is the only member of the so-called Five Eyes intelligence alliance (Australia, Canada, New Zealand, the United Kingdom, and the United States) that has not made a determination on the use of Huawei equipment. Prime Minister Justin Trudeau's government is reportedly studying the details of the UK decision before making its own choice.[ix]

Executive Branch Strategies/Policies to Address the Problem

The Obama Administration

The 2014 Quadrennial Defense Review (QDR)[x] released by the Obama Administration in March of that year was one of the first USG documents to highlight the fact that innovation must become a strategic priority given that the spread of other sophisticated technologies to potential adversaries poses new security challenges. The QDR stated that DOD must achieve affordable programs and increase productivity in defense acquisition by "controlling costs, incentivizing productivity and innovation in industry and government, eliminating unproductive processes and bureaucracy, promoting effective competition, improving tradecraft in contracted acquisition of services, and improving the professionalism of the total acquisition workforce."

The document highlighted the fact that the global technology landscape is changing with U.S. technological superiority being challenged by "increasingly capable and economically strong potential adversaries that are likely developing and fielding counters to some or all of the key technologies on which the United States has come to rely." If the United States is to maintain technical and military superiority, it will be necessary for DOD to develop "new capabilities, tactics, techniques, and procedures to continue to be effective ... [and] ensure that technological superiority is maintained in areas most critical to meeting current and future military challenges."[xi]

Then-Secretary of Defense Ash Carter expanded on many of these QDR themes in a speech at Stanford University on April 23, 2015.[xii] Secretary Carter stated that threats to U.S. security and military-technological superiority are proliferating and diversifying and that "high-end military technologies long possessed by only the most advanced foes find their way into the arsenals of both non-state actors and previously much less capable militaries." At the same time China and Russia are undertaking comprehensive military modernization programs to close the technology gap with the United States.

He underscored the need to work more closely with commercial startups because they are "the leading edge of commercial innovation" adding that DOD must bring the private sector's best practices back into the Defense Department. Too often, DOD forfeits an innovative idea or needed capability because "the Pentagon bureaucracy was too slow to fund something, or we weren't amenable to working with startups, as we should be."

To help counter these trends, Secretary Carter announced the creation of the Defense Innovative Unit Experiment (discussed in greater detail in a subsequent section) designed to strengthen existing relationships and build new ones. While admitting that non-traditional, commercial startups cannot provide all of DOD's technological needs (e.g., they will never produce hypersonic missiles or F-35 fighters), "there are many areas where the potential in leveraging commercially-driven technology is so huge, that we have to embrace it going forward."[xiii]

The Trump Administration

The December 2017 *National Security Strategy of the United States* (NSS)[xiv] and *National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, released in January 2018, provide insights into the Trump Administration's views on the shifting global R&D environment and set forth a framework for its policies to safeguard U.S. technological preeminence and battlefield ascendancy.

The National Security Strategy

In a section entitled "Lead in Research, Technology, Invention, and Innovation," the NSS states that "To maintain our competitive advantage, the United States will prioritize emerging technologies critical to economic growth and security." The private, commercial sector is the source of a range of technologies that DOD depends upon to carry out national security missions. These include advanced computing, big data analytics, artificial intelligence, robotics, autonomous technologies, additive manufacturing, new materials, nanotechnology, and miniaturization, technologies that will help ensure that the United States is able to fight and win future conflicts.

The NSS sets forth four "priority actions" required to sustain the competitive advantage of the United States:

1. Increase understanding in DOD – and other USG agencies – about how globalization is shaping worldwide science and technology trends and "how they are likely to influence – or undermine – American strategies and programs."
2. Augment collaboration with industry and academia and the recruitment of technical talent creating "easier paths for the flow of scientists, engineers, and technologists into and out of public service."

3. Utilize technical expertise and R&D capabilities of the private/commercial sector more effectively. DOD – and other USG agencies – "will establish strategic partnerships with U.S. companies to help align private sector R&D resources to priority national security applications."
4. To "regain the element of surprise" and deploy technologies "at the pace of modern industry" DOD and USG agencies must "shift from an archaic R&D process to an approach that rewards rapid fielding and risk taking."[xv]

In a related section called "Promote and Protect the U.S. National Security Innovation Base [NSIB]," the NSS states that competitors of the United States such as China are pilfering U.S. intellectual property valued at hundreds of billions of dollars. Actors are also gaining access to U.S. technologies, experts, and trusted foundries (for the secure production of microelectronics)[xvi] by largely legitimate means to "fill their capability gaps and erode America's long-term competitive advantages." Consequently, the NSIB – defined as the U.S. network of knowledge, capabilities, and people including academia, the national laboratories, and the private sector – is crucial for U.S. national security and prosperity and must be defended.

As priority actions to safeguard the NSIB the United States should:

1. Develop a USG capability to "integrate, monitor, and better understand the national security implications of unfair industry trends and the actions of our rivals" and share this information with the private sector and academia.
2. Reduce the unlawful theft of U.S. public- and private-sector technology and technical knowledge by foreign competitors and "explore new legal and regulatory mechanisms to prevent and prosecute violations."
3. Review the procedures for acquisition of visas to decrease economic theft by non-traditional intelligence collectors while also "acknowledging the importance of recruiting the most advanced technical workforce to the United States."
4. Expand the focus of the USG beyond protecting the U.S. network infrastructure to include safeguarding the data stored and transmitted on those networks and "encourage practices across companies and universities to defeat espionage and theft."[xvii]

The National Defense Strategy

Published over a year after the NSS, the Pentagon's *National Defense Strategy* (NDS)[xviii] elaborates and builds upon several of the ideas and themes set forth in the NSS. The NDS reiterates the significant impact rapid technological advancements originating from the commercial sector have on the security environment and states that ready access to the most advanced, applicable commercial technologies is crucial.

A section entitled "Challenges to the U.S. Military Advantage" is particularly relevant. It discusses the: changed global environment and character of war; rapid rate of innovation; growing dependence of DOD on commercial technologies and capabilities; increased availability of these commercial technologies globally to state and non-state adversaries; erosion of U.S. technological advantage; and need for cultural change within DOD to

incorporate commercial technologies, best practices, and speedier development and fielding schedules.

The NDS states that for several decades the United States has enjoyed superiority in all operating domains. This is no longer true, however: "Today, every domain is contested – air, land, sea, space, and cyberspace." In addition, the NDS states that the security environment is impacted by rapid technological advancements and that the "drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed," factors that "will change society and, ultimately, the character of war."

Similar to the NSS, the NDS states that sustaining our technological advantage requires structural and cultural changes within the Defense Department to support innovation and the protection of the U.S. NSIB. DOD must dramatically accelerate and streamline the process by which commercial technology is sourced and integrated across the U.S. defense enterprise to ensure our technological lead.

In a frank assessment of a major development and procurement flaw within DOD, the NDS declares that:

"The current bureaucratic approach, centered on exacting thoroughness and minimizing risk above all else, is proving to be increasingly unresponsive. We must transition to a culture of performance where results and accountability matter… Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting. Current processes are not responsive to need; the Department is over-optimized for exceptional performance at the expense of providing timely decisions, policies, and capabilities to the warfighter."[xix]

Specific Measures to Address the Situation

The Administration, DOD, Congress, and the major defense companies have taken a number of steps to implement the strategies outlined in the documents above designed to make DOD and the broader defense enterprise more effective in the development and acquisition of advanced technologies. These include changes in the organization of the Pentagon's R&D activities, creation of new acquisition policies and authorities, attempts to change the DOD acquisition culture and increase the speed of fielding systems, establishing a presence in key U.S. technology hubs, and the establishment of venture capital entities within DOD and major defense contractors to identify and encourage commercial startups to work with the Defense Department and the defense industry.

The Defense Innovation Unit

As noted above, the growing concern that DOD was not incorporating the technological advances being produced in the commercial sector led then-Secretary of Defense Carter to create the Defense Innovation Unit Experimental (DIUx) in April 2015. The establishment of DIUx underscored the fact that startup technology companies and other commercial firms were far outpacing the DOD establishment in producing needed advanced, innovative technologies. Not surprisingly, the first DIUx office was established in Silicon Valley to tap into the companies producing a range of dual-use technologies there. A year later DIUx offices were opened in the high-tech hubs of Boston, MA and Austin, TX, and in 2018, in Washington, D.C.

With these new centers DIUx also restructured its organization to one based on a partnership-style leadership model similar to venture capital firms. However, unlike venture capital firms, DIUx provides nondilutive capital to the commercial firms (i.e., DIUx does not require equity [partial ownership of the commercial firm] in exchange for funding).

DIUx's mission is to strengthen U.S. national security by accelerating the incorporation of commercial technology throughout the U.S. military and expanding the U.S. NSIB. DIUx partners with DOD organizations, the military services, and combatant commands to carry out prototype projects and rapidly field commercial solutions that address national security challenges.

A key goal is also to encourage non-traditional suppliers to work with DOD to access their advanced technologies and provide solutions to national defense problems. DIUx focuses on five key technology areas in which the commercial sector outpaces the U.S. military sector. These are artificial intelligence, autonomy, cyber, human systems, and space.

As will be described in greater detail below, a key element of DIUx's approach (and that of similar DOD/national security efforts) is the utilization of other transaction authority (OTA) agreements to facilitate the participation of non-traditional defense companies and startups in DOD efforts by easing the complex contracting requirements and stipulations of the Defense Department. DOD's daunting and lengthy Federal Acquisition Regulation (FAR) contracting process discourages many commercial startups and potential non-traditional suppliers from seeking work with the Defense Department.

Unlike the traditional DOD contracting-award process which normally takes over 18 months to complete, DIUx seeks to transition from problem identification to the award of a prototype contract within 60 to 90 days. The length of typical DIUx prototype projects, which are administered under OTAs, is 12 to 24 months. When completed, successful prototype efforts may move to follow-on production via another OTA or through a FAR-based contract.

DIUx has successfully transitioned into the Trump Administration. Highlighting its importance and DOD's need to become far more adept at accessing commercial technologies, in 2018 the organization underwent a re-branding, dropping "Experimental" from its name to become the Defense Innovation Unit or DIU. According to then-Secretary of Defense Patrick Shanahan, "Removing 'experimental' reflects DIU's permanence within the DOD … and that DIUx has generated meaningful outcomes for the Department and is a proven, valuable asset. DIU remains vital to fostering innovation across the Department and transforming the way DOD builds a more lethal force."[xx]

A key challenge DOD confronts as it attempts to encourage greater participation in defense-contracting opportunities by the commercial community is the fact that some high-tech companies in Silicon Valley and elsewhere in the United States have an anti-defense culture. Several factors account for this suspicion of DOD and reluctance to work with it.

These include: DOD's bureaucratic and time-consuming contracting regime; a desire to sell their products abroad, particularly to China, and thus not wanting to appear too close to the USG/DOD; and perhaps most importantly, the continuing fallout and resentment of many high-

tech employees related to Edward Snowden's 2013 revelations about spying on U.S. high-tech companies by the National Security Agency.

DOD's Project Maven is an illustrative case study of the anti-defense culture percolating in some high-tech companies. Google was supplying AI tools to DOD for the rapid analysis of large volumes of drone video to support the U.S. anti-terrorism mission but pulled out of the contract because its employees protested working with the Pentagon. Paradoxically, similar employee opposition did not emerge when Google contracted with China on several projects allowing Beijing access to some of Google's AI technologies.[xxi]

This anti-defense bias puts the United States at an inherent disadvantage with countries such as China. The challenge will be how to garner necessary support from the high-tech business community to ensure that the United States can access/leverage those commercially developed technologies.

The USG and DOD will need to make pursuing defense opportunities a more attractive and profitable option for commercial companies. This requires reducing the anti-defense culture by outreach underscoring that DOD and commercial companies have shared values including net neutrality and a free and open Internet as well as keeping the United States economically and militarily strong; providing incentives to high-tech firms both by relaxing burdensome contracting regulations and making more widespread use of OTAs; and protecting the company's intellectual property.

Open Campus Initiative and Army Venture Capital Initiative

The Army's Open Campus Initiative (OCI)[xxii] of the U.S. Army Research Laboratory (ARL) is an attempt to establish long-term science and technology (S&T) partnerships via the placement of Army R&D personnel in S&T hubs to expand its presence both locally and globally and increase collaboration with the U.S. NSIB. It seeks to develop a S&T ecosystem fostering advances in basic- and applied-research areas germane to Army operations.

These include computational sciences; materials research; sciences for maneuver; information sciences; sciences for lethality and protection for soldiers and army platforms; and human sciences, including human-physical interface, human-human interface and human-technology interface.[xxiii]

Through the OCI, ARL scientists and engineers work collaboratively with visiting scientists and as visiting researchers at collaborators' institutions. The global academic community, industry, small businesses, and other USG research laboratories benefit from this engagement through collaboration with ARL's specialized staff and technical facilities. This collaboration develops research networks to explore complex problems, and exposes scientists, engineers, professors, and students to realistic research applications.

The Army Venture Capital Initiative (AVCI)[xxiv] is a venture capital activity of the U.S. Army and Department of Defense to invest in cutting-edge technologies. Chartered by Congress and established in 2002, the AVCI supports venture-funded companies developing innovative technologies needed by the Army. It supports technology startups that have traditionally been overlooked by DOD or which have had little interest in working with the Defense Department.

The goal of AVCI is to fast-track product development and deliver advanced warfighting capabilities. The AVCI, in combination with investments by private venture capital firms, helps firms develop products needed by Army warfighters. For each dollar AVCI invests in a company, on average the private venture capital community invests more than $22.

In-Q-Tel

In-Q-Tel (IQT)[xxv] is a not-for-profit strategic investor that accelerates the development and delivery of cutting-edge technologies to national security agencies. IQT was created in 1999 to ensure that U.S. intelligence agencies had access to innovative technologies from the startup community to help protect and preserve U.S. security. The senior leadership of the Central Intelligence Agency recognized that technological innovation had shifted primarily from USG R&D and large organizations/major defense companies to entrepreneurs in the startup community who were developing requisite technologies both more rapidly and less expensively.

IQT funds startup companies whose emerging technologies show promise in critical areas such as data analytics, cyber security, AI/machine learning, ubiquitous computing, IT solutions, communications, materials/electronics, commercial space, power and energy, and biotechnology. IQT attempts to bridge the gap between the diverse technology needs of its government partners (the intelligence community and increasingly DOD), the innovations of the commercial startup sector, and the venture community that funds those startups. IQT's access to and understanding of these varied communities enables it to make meaningful investments.

IQT first assesses a company's technology against the requirements of its partners' mission needs, compares alternate approaches and then validates the company's technical claims. At the same time, IQT evaluates the company's business plan and management team to determine the firm's potential for long-term success. It is looking for "ready-soon" technology, i.e., off-the-shelf products that can be modified, tested, and delivered for use within 6 to 36 months.

If IQT makes an investment, it collaborates with the company and the partner USG agencies to finalize a work program and expediate a successful technical outcome. IQT's approach provides several advantages including rapid product development; valuable product enhancements; and lower initial and long-term costs to the national security community. An investment in a startup by IQT is often viewed as a stamp-of-approval, frequently resulting in additional investments by private venture capital firms.[xxvi] Over the past two decades IQT has invested in hundreds of companies and startups.

Defense Innovation Board

Another effort designed to encourage greater DOD use of commercial technologies was the establishment in in 2016 of the Defense Innovation Board (DIB) as an independent federal advisory committee. Dr. Eric Schmidt, former Executive Chairman of Alphabet, Inc., chairs the DIB.

DIB members include prominent business leaders, scholars, entrepreneurs, inventors, scientists, and technologists from leading U.S. technology companies, venture capital firms, research institutes, and universities, appointed by the Secretary of Defense. Members provide guidance and recommendations to the Secretary of Defense and senior DOD leadership on

innovative approaches to address future challenges focusing on people and culture, technology and capabilities, and practices and operations.

Simplifying DOD Contracting: Other Transaction Authority Agreements

Increasingly cognizant of the need to foster greater participation by innovative commercial startups and non-traditional suppliers in DOD contracting opportunities, Congress has increased the Defense Department's authority to utilize other transaction authority agreements. This contract vehicle is a legally binding agreement providing DOD and other federal agencies with increased contracting flexibility because OTAs are not subject to the cumbersome and time-consuming Federal Acquisition Regulation contracting process, the USG's principal set of rules governing USG procurement.

OTAs can be utilized for several different types of contracts. However, they are particularly well suited for research and development efforts. In contrast to a FAR contract for purchase of commodities or services, R&D contracts seldom have a known result or outcome. Frequently, OTA contracts are used to develop a prototype for testing new solutions to problems. As noted earlier, this is primarily the case with DIU contract engagements.

OTAs encourage both the contractor and the contracting agency to work together to determine which requirements will be most beneficial for the execution of the contract. It helps the government to learn new acquisition approaches and best practices, especially from non-traditional technology providers. OTAs facilitate this collaboration, rather than forcing agencies and contractors to abide by the often-rigid requirements of FAR contract vehicles.

As noted, the onerous FAR process has been a major impediment discouraging many startups and non-traditional suppliers from competing for contracts and working with DOD. OTAs, in sharp contrast to FAR's complicated requirements, allow DOD to negotiate agreements explicitly tailored to the needs of the project and its participants. As a consequence, the use of OTAs has grown significantly in the federal government over the past few years because of their ability to help federal agencies rapidly incorporate new technologies required to ensure the success of DOD's increasingly complex missions.

In fact, according to a recent report, the use of OTAs to fund industry "now exceeds funding to industry obligated through the traditional weapon system development pipeline (i.e. the FAR process)." The report also states that approximately two-thirds of OTA expenditures "goes to non-traditional R&D firms, while the traditional weapon systems development pipeline is dominated by traditional defense companies."[xxvii]

Major U.S. Defense Companies and their Venture Capital Arms

Large U.S. defense contractors are also increasingly aware of their need to leverage/access the technologies developed in the startup community. Over the past few years, several large defense contractors including Boeing, Lockheed Martin, and BAE Systems, Inc. have formed venture capital (VC) divisions (HorizonsX, Ventures, and FAST Labs, respectively) within their companies. Hopefully, these activities will contribute to DOD's efforts to tap more effectively into the commercial innovation sector.

Defense executives are looking beyond their own R&D laboratories for innovative capabilities and technology breakthroughs. They hope their VC divisions will harvest technology and

capabilities from their startup investments applicable to its own weapon systems and platforms. Defense industry officials agree that, like the bureaucratic environment in DOD described earlier, large defense contractors have become risk adverse and resistant to change which obstructs the adoption of new technologies and approaches.

In particular, these executives believe technologies will emerge in the commercial-start-up sector that will push the defense industry to more automation and efficiency. "Low-cost manufacturing and efficiency are the Holy Grail in the defense industry … [and will lead to] rapid cost reduction, rapid evolution of the technology." They also hope that their VC investments give established defense companies an infusion of entrepreneurial culture.[xxviii]

Defense executives first became aware of the disruption startups could pose to their businesses and the consequent need to access the commercial sector for advanced technologies when, in April 2016, Elon Musk's SpaceX won its initial space launch-vehicle contract from the U.S. Air Force and DOD. This award brought to an end the decade-long monopoly of United Launch Alliance, a Boeing-Lockheed Martin joint venture, for space launch services.[xxix]

Conclusions

Today, most advanced technologies with direct military/defense applications – i.e., dual-use technologies – are developed and produced by the commercial sector. R&D funding in the U.S. (and foreign) commercial sector now far exceeds R&D spending by DOD. These two factors have significant implications for how DOD acquires such technologies and its ability to preserve military superiority.

The U.S. military's technological advantage is eroding because these advanced, dual-use technologies are becoming more widely available on a global basis. Although some progress has been made, DOD has been slow to leverage dual-use technologies including Fourth Industrial Revolution technologies such as artificial intelligence, cloud computing, quantum computing, autonomy, robotics, 3D printing, the Internet of Things, and advanced wireless technologies/networks/5G. This trend is accelerating.

Its growing capabilities and strategy to achieve global technological dominance make China our leading competitor. Unlike in the United States, few political, legal, economic, or cultural roadblocks exist in China to prevent collaboration across such sectors as industry, academia, research labs, the military, and government. This allows the Chinese government to direct technology development priorities and funding.

The U.S. government, DOD, Congress, and traditional defense industry suppliers need to develop strategies, enact policies, make organizational changes, shed long-held cultural biases and outdated business practices, and encourage non-traditional high-tech commercial firms to work with DOD. DOD needs to develop a more integrated acquisition structure to include closer collaboration and partnership with the government defense/national security enterprise, with the commercial sector, traditional defense suppliers, and academia. These efforts are essential if the U.S. defense enterprise is to benefit more fully from leading-edge commercial technologies.

As the Trump Administration's National Security Strategy and National Defense Strategy acknowledge, current DOD acquisition processes do not provide timely decisions, policies, and

capabilities to the warfighter. Both documents describe the shifting global research and development environment. The United States can best ensure U.S. technological preeminence by:

- Identifying the various impediments within DOD and the government for accessing commercial-sector technologies and capabilities more effectively;
- Implementing structural and cultural changes within the Defense Department to support innovation by streamlining the integration of commercial technology across the U.S. defense/national security enterprise; and,
- Creating strategic partnerships to align private sector R&D resources to priority defense/national security applications.

In support of these efforts, important specific initiatives have already been undertaken that provide a basis for further action. These include:

- Changes in the organization of the Pentagon's R&D activities;
- Creation of new acquisition policies and authorities;
- Actions to change the DOD acquisition culture and increase the speed of fielding systems;
- Establishing a presence in key U.S. technology hubs;
- Establishment of venture capital entities within the government and DOD (e.g., In-Q-Tel, the Defense Innovation Unit, and Army Venture Capital Initiative) and in major defense contractors to identify technologies and encourage commercial startups to work with DOD and the defense industry; and,
- Use of other transaction authority agreements to facilitate the participation of non-traditional defense companies and startups in DOD efforts. OTAs allow speedier contract awards by relaxing/doing away with many of DOD's complicated contracting requirements which discourage commercial startups and potential non-traditional suppliers from working with the Defense Department.

A key challenge facing DOD in gaining greater commercial sector participation in defense projects is an anti-defense culture in some high-tech firms as evidenced by Google's exit from DOD's Project Maven, a program to use artificial intelligence to help track down terrorists. This anti-defense bias puts the United States at an inherent disadvantage with countries such as China. To rectify this situation and to make pursuing defense opportunities an attractive and profitable option for commercial companies, several priority efforts should be undertaken including:

- Mitigating high-tech's anti-defense culture by outreach underscoring that DOD and commercial companies have shared values in helping to ensure a strong U.S. economy and defense;
- Incentivizing high-tech companies by easing the onerous DOD contracting regulations and utilizing OTAs more frequently; and,
- Protecting a company's intellectual property.

Endnotes

[i] *The Global Research and Development Landscape and Implications for the Department of Defense*, Congressional Research Service, updated November 8, 2018, pp. 4-6. See https://fas.org/sgp/crs/natsec/R45403.pdf.

[ii] The Fourth Industrial Revolution or 4IR is characterized by the fusion of the digital, biological, and physical worlds, as well as the growing utilization of new technologies such as artificial intelligence, cloud computing, robotics, 3D printing, the Internet of Things, and advanced wireless technologies, among others. See Devon McGinnis, "What is the Fourth Industrial Revolution?" *Salesforce Blog*, December 20, 2018 at https://www.salesforce.com/blog/2018/12/what-is-the-fourth-industrial-revolution-4IR.html.

[iii] Ibid, 10.

[iv] *Made in China 2025*, China State Council, July 7, 2015. See http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf.

[v] "Full Translation: China's 'New Generation Artificial Intelligence Development Plan,'" *New America*, August 1, 2017. See https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

[vi] Daniel S. Hoadley and Nathan J. Lucas, "Artificial Intelligence and National Security," CRS Report, April 26, 2018. See https://www.a51.nl/sites/default/files/pdf/R45178.pdf.

[vii] Michael Brown and Pavneet Singh, China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation, Defense Innovation Unit Experimental (DIUx), January 2018. See https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

[viii] David Sanger, "Trump Wants to Wall Off Huawei, but the Digital World Bridles at Barriers," *New York Times*, May 27, 2019. See https://www.nytimes.com/2019/05/27/us/politics/us-huawei-berlin-wall.html.

[ix] Katharina Buchholz, "Which Countries Have Banned Huawei?," January 30, 2020. See https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/.

[x] The *Quadrennial Defense Review 2014*, Department of Defense, March 2014. See https://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

[xi] Ibid, 25.

[xii] "Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity," The Drell Lecture at Stanford University delivered by Secretary of Defense Ash Carter, April 23, 2015. See https://archive.defense.gov/speeches/speech.aspx?SpeechID=1935.

[xiii] Ibid.

[xiv] *National Security Strategy of the United States*, December 2017. See https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[xv] Ibid, 20-21.

[xvi] The Defense Department and the National Security Agency (NSA) initiated the Trusted Foundry Program for microelectronics in 2004 to reduce the vulnerabilities associated with the increasing reliance on foreign manufacturers for microelectronics and to meet low-volume government needs. A sole-source contract was awarded to the IBM Corporation, the only U.S.-based company able to meet DOD and intelligence community needs for trusted leading-edge microelectronics at that time. In 2006, the Trusted Foundry Program was expanded to include firms offering mature technologies and became the "trusted supplier program." See "Trusted Defense Microelectronics: Future Access And Capabilities Are Uncertain," GAO Report, October 2015, p. 2 at https://www.gao.gov/assets/680/673401.pdf.

[xvii] *National Security Strategy of the United States*, pp. 21-22.

[xviii] *Summary of the 2018 National Defense Strategy*. See https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[xix] Ibid, 10.

[xx] "DIUx Name Changing to Reflect Permanence," *MeriTalk*, August 10, 2018. See https://www.meritalk.com/articles/diux-name-changing-to-reflect-permanence/.

[xxi] See Hoadley and Lucas, "Artificial Intelligence and National Security," CRS Report; Drew Harwell, "Google to drop Pentagon AI contract after employee objections to the 'business of war'," *Washington Post*, June 1, 2018 at https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/google-to-drop-pentagon-ai-contract-after-employees-called-it-the-business-of-war/; and "When Technology Can Be Used To Build Weapons, Some Workers Take A Stand," *NPR's All Things Considered*, May 13, 2019 at https://www.npr.org/2019/05/13/722909218/when-technology-can-be-used-to-build-weapons-some-workers-take-a-stand.
[xxii] "Open Campus." See https://www.arl.army.mil/opencampus/?q=Introduction.
[xxiii] "Army Research Laboratory Open Campus," Press Release. See https://research.umd.edu/arl.
[xxiv] Army Venture Capital Initiative Website. See https://armyvci.org/.
[xxv] In-Q-Tel Website. See https://www.iqt.org/.
[xxvi] Paul Szoldra, "14 cutting edge firms funded by the CIA," *Business Insider*, September 21, 2016. See https://www.businessinsider.nl/companies-funded-by-cia-2016-9/.
[xxvii] Seamus P. Daniels, Mark F. Cancian, Andrew P. Hunter, Thomas Karako, Wes Rumbaugh, and Todd Harrison, "What to Look for in the FY 2021 Defense Budget Request," *Defense360*, CSIS, p. 4. See http://defense360.csis.org/wp-content/uploads/2020/02/FY-2021-Preview-Brief_FINAL.pdf.
[xxviii] Doug Cameron, "Defense Industry Adds Venture Capital to Its Arsenal," *Wall Street Journal*, July 5, 2018. See https://www.wsj.com/articles/defense-industry-adds-venture-capital-to-its-arsenal-1530792001.
[xxix] Ibid.

The Institute for Foreign Policy Analysis

http://www.ifpa.org

Robert L. Pfaltzgraff, Jr., President
RLP@ifpa.org

Jack Kelly, Senior Staff
kell@ifpa.org

March 13, 2020 Report

The *IFPA National Security Update* series addresses critical current and emerging national, international, and economic security and foreign policy issues facing the United States. IFPA *Updates* are made available to members of the executive branch, the military services, members of Congress and their staff, and the broader national security public policy community.

The Institute for Foreign Policy Analysis, Inc. (IFPA) develops innovative strategies for new security challenges. IFPA conducts studies and produces reports, briefings, and publications. We also organize seminars and conferences. IFPA's products and services help government policymakers, military and industry leaders, and the broader public policy communities make informed decisions in a complex and dynamic global environment. To find out more about IFPA's work and publications, visit www.IFPA.org.

Institute for Foreign Policy Analysis, PO Box 390960, 770 Massachusetts Ave., Cambridge, MA 02139