Rightly Scaled, Carefully Open, Infinitely Agile: Reconfiguring to Win the Innovation Race in the Intelligence Community

House Permanent Select Committee on Intelligence

Strategic Technologies and Advanced Research (STAR) Subcommittee

Chairman Rep. Jim Himes
Ranking Member Rep. Chris Stewart

ACKNOWLEDGMENTS

This report represents the culmination of the House Permanent Select Committee on Intelligence's Subcommittee on Strategic Technologies and Advanced Research efforts during the 116th Congress to understand how the Intelligence Community pursues innovation, and would not have been possible without the valuable contributions of many individuals and organizations.

While this report was written by the Subcommittee, the entire membership of HPSCI and the Committee's staff had a hand in it, in particular Raffaela Wakeman, Conrad Stosz, Thomas Eager, Amanda Rogers Thorpe, Krishna Pathak, Kelsey Lax, William Wu, Steve Keith, and Andrew House. In addition, I am also thankful for the collaboration with my fellow Subcommittee Chair Eric Swalwell and his Subcommittee Staff Director Kathy Suber, given the import of human capital management and security clearances to the subject of this report. And from my personal office staff, I'd like to thank Jessica Hagens-Jordan, Patrick Malone, and Elena Radding.

In addition to the dozens of career intelligence professionals we learned from, I am grateful for the expertise rendered by the dedicated public servants and thought leaders inside and outside government we met with to help us understand how the United States pursues innovation, and how we can empower the Intelligence Community to be ever more agile and open. In particular, my sincere thanks go to the superb witnesses at our open hearing on February 12, 2020: Chris Darby, DJ Patil, Nick Sinai, and Maria Zuber.

Finally, the publication of this report does not signify the conclusion of the Subcommittee's focus on innovation in the Intelligence Community. We will continue to poke, prod, and press for the adoption of our recommendations, and where we identify additional changes that warrant reform, we will pursue those, as well.

Jim Himes
Subcommittee Chairman

TABLE OF CONTENTS

Executive Summary

From our nation's founding moment, innovation has been an essential ingredient of American prosperity and national security. During World War II, the threat of a Nazi atomic bomb prompted a federal commitment to basic research that transformed every element of American life, including establishing American technological pre-eminence. Today, neither that pre-eminence, nor the commitment that fueled it, are unchallenged. We live in a dramatically changed world. Innovation is happening almost everywhere, including in the laboratories of our adversaries. Threats are dispersed; terrorism, cybercrime, even a radiological or biological attack do not require nation-state sponsorship. And just as nuclear technology emerged to change the world 75 years ago, artificial intelligence, quantum computing, biosynthesis and other new technologies promise to reorder the global chessboard and change the lives of everyone on the planet.

The question for U.S. policymakers, and the subject of this report, is whether the United States will lead in the development of these technologies or whether we will follow, and instead merely read about their unpredictable effects in the media. Our national security depends on choosing the former path, as does our economic prosperity and our traditional leadership role in the development of the global norms, rules and institutions that disperse technology's benefits and constrain its destructive potential.

Like every element of our government, the U.S. Intelligence Community ("IC") has a crucial role to play in this endeavor. It brings to that role unique assets: robust funding, exceptional people, and technology that is the stuff of Hollywood thrillers. But its innovative capacity is also constrained by necessary secrecy, compartmentalization and rules and a culture that often punishes risk and cements the status quo.

Over the last 18 months the Subcommittee on Strategic Technologies and Advanced Research has undertaken a study of existing thought leadership and engaged with IC leaders and experts. This report presents the Subcommittee's views and recommendations and identifies those that are best suited for legislative action, executive branch initiatives, or further study. While our jurisdiction is limited to the IC, we have drawn liberally on reviews of other government elements, especially the Department of Defense. And our recommendations must, if they are to be successful, be a part of a whole-of-government approach.

The recommendations of the Subcommittee focus on five specific areas. The first three are the critical components of innovation: money, people, and the environment in which they come together. The fourth focuses on strategic vision and coordination. The fifth focuses on the traditional American role of leading in the development of international norms. The Subcommittee believes this is critical because technological races rarely stay "won" for long. Technology disperses. Always. So true national security requires rules, predictability and transparency into how, when and why these tools are used.

Our recommendations include:

Get the Money Right:

- Expand the Federal Commitment to Basic Research
- Recalibrate Spending on R&D

Get the People Right:

- Broaden Targeted Hiring Authorities
- Expand Retention Incentives
- Create a STEM Fellowship Program in the IC
- Engage with Educators
- Explore Talent Exchanges
- Accelerate Security Clearance Reform
- Reconsider Whether All IC Personnel Require a Security Clearance
- Fix Immigration to Get and Keep Talent

Get the Environment Right:

- Invest in Private Sector Partnerships
- Learn Software Development Fast
- Rethink Acquisition Procedures and Culture
- Invest in Open Source Intelligence
- Leverage and Nurture the Federal Labs
- Collaborate with Foreign Partners
- Congress, Heal Thyself

Improve IC Strategy and Vision:

- Focus IC Strategic Leadership
- Establish an Intelligence Innovation Board

Lead in the Development of Norms and Standards

The Subcommittee notes that the national security innovation race is often framed as a competition with China. While this is an overly narrow view, it is true that China has dramatically increased its commitment to innovation in terms of money, strategic coordination and methods both legal and illegal to become a near-peer to the United States in technological capability. So we note, with some satisfaction, that our recommendations are generally not calls for the hierarchy, direction and centralized control that characterize Chinese innovation efforts. Instead, they reflect the ideas of openness, flexibility and agility that gave rise to American innovative success from Los Alamos to Silicon Valley.

As Eric Schmidt, former CEO of Google and the first Chairman of the Defense Intelligence Board, noted, we may not have an innovation problem, we may have an "innovation adoption" problem. The ideas are out there, and many of them have been for some time. Now is the time for their adoption. Our tradition of technological leadership and the security that follows is at stake.

I. INTRODUCTION

In 1938, two chemists in Nazi Germany, Otto Hahn and Fritz Strassmann, bombarded uranium with neutrons to discover nuclear fission. The explosive energy produced, and the fact that it had occurred in Nazi Germany, caused several European physicists, including Albert Einstein, to write to U.S. President Franklin D. Roosevelt about the possibility of a terrifying new bomb, capable of unprecedented destruction. As he read Dr. Einstein's warning, President Roosevelt understood that certain technological advancements would be capable of both improving life and altering history, possibly catastrophically.

Einstein warned the President of the threat of what we would call today "game changing" technology. In response to this warning, the Manhattan Project – and a broad commitment to American technological innovation – was born. The Manhattan Project accelerated the Allies past Nazi Germany to develop an atomic bomb, the weapon that ultimately brought the war against Japan to an abrupt end. For generations since, people have toyed with the dark counterfactual question of what might have happened had Nazi Germany won that technological race.

Vannevar Bush, the director of the Office of Scientific Research and Development – which oversaw the Manhattan Project – and "father" of America's official commitment to innovation, saw basic research as more than just a means to protect national security. In 1945, he noted that "Advances in science when put to practical use mean more jobs, higher wages, shorter hours, more abundant crops, more leisure for recreation, for study, for learning how to live without the deadening drudgery which has been the burden of the common man for ages past."[1]

American innovation in the 75 years since Bush's observation has been a partnership between government-sponsored basic research and a private sector finding applications and commercializing that research.[2] The ubiquitous iPhone is just one example of this partnership: almost all of the technology enabling its wondrous applications – semiconductors, GPS-based location services, voice recognition technology, and the Internet itself – was initially researched in government laboratories.

The United States' strategic decision to propel basic scientific exploration through sustained funding – even, or *especially* when the practical application of that research was unclear – sustained successes in the post-World War II era. Often, those funding decisions led to consequential advantages to U.S. national security.[3]

Today, however, two trends have converged to threaten U.S. national security and specifically to erode the relative effectiveness of the IC. First, the United States and its adversaries are in a Manhattan Project-like race to develop several game-changing technologies, including high-performance and quantum computing, artificial intelligence ("AI"), and biosynthesis. Second, the United States' historical position as an uncontested leader in basic research has, since the end of the Cold War, been fading fast.[4] The United States is no longer the clear leader.

China, in particular, poses a significant threat. Quantitatively, China now rivals the United States on research and development ("R&D") spending, accounting for 26% of global spending compared to the United States' 28%.[5] This near parity is a result of the Chinese strategy of massive coordinated investment in designated technological areas.[6] In some technologies, particularly biotechnology, China may be a peer or near-peer to the United States.[7]

In the last several years, report after report has sounded the alarm over America's declining edge in scientific and technological ("S&T") R&D. In 2013, the congressionally-established National Commission for the Review of the Research and Development Programs of the United States Intelligence Community ("the Commission") released a comprehensive report and recommendations on the topic.[8] Several of the Commissioners remain sitting Members of Congress, serving on the Senate Select Committee on Intelligence ("SSCI") and the House Permanent Select Committee on Intelligence ("HPSCI").

Since the Commission's report, many think tanks, including the Council on Foreign Relations ("CFR"), the Center for Strategic and International Studies ("CSIS"), the Center for a New American Security ("CNAS"), and the Center for Security and Emerging Technology ("CSET"), have voiced their concern over our eroding lead in global R&D. The recommendations of the Commission and the think tanks are remarkably consistent, but they have received insufficient attention from legislators and other policy makers. Appendix A summarizes many of these reports' recommendations.

Over the last year, the Subcommittee explored the IC's strengths and shortcomings in technological innovation. Our intent was not to duplicate the work of the aforementioned studies but rather to look at the IC's technological innovation from the inside and to offer fresh thinking on what can and should be done by legislators and policymakers.

Because of the Subcommittee's jurisdiction, we focused particularly on the IC as it contributes to national security. National security, of course, is an abstraction, distant from the people, institutions and cultures that promote (or inhibit) innovation. The IC is in some ways radically different from the Department of Defense ("DOD"), with its own set of missions, cultures and personnel, even as it overlaps in many of those missions, departments and challenges. Our report focuses on innovative capacity in the IC specifically, even as we considered some particularly relevant challenges and initiatives undertaken by others, including the DOD.

Innovation, too, is an abstraction. It is the product of a complicated mixture of money, people, and environment as well as intangible characteristics like genius, inspiration and culture. Getting these factors right leads to trillions of dollars of wealth creation in Silicon Valley or the development of a war-winning weapon at Los Alamos. Getting these factors wrong leads to "also-ran" status, not an enviable position in the realm of national security.

This report makes recommendations with respect to each of these key inputs: money, people and environment. Taken together, these recommendations suggest that the U.S. does not necessarily need to "beat China at its own game" of more centrally directed, hierarchical, planned innovation. Instead, we need to do better in the distinctly American direction of openness, flexibility and agility.

To carry out our research, surface relevant findings, and develop recommendations, the Subcommittee met with numerous experts and practitioners both inside and outside of government and reviewed selected literature on the nexus of technology and national security. Recognizing the importance of identifying unconventional or novel ways for the IC to harness emerging technology, the Subcommittee devoted considerable attention to capturing insights from credible voices beyond Washington, including prominent representatives from venture capital, academia, industry, and from the startup community. Appendix B contains a description of the Subcommittee's engagements.

We must act now. Studies, reports and commissions have warned for decades about the risks to national security from the steady erosion in our innovative capacity. Those risks are no longer abstract or speculative. They are upon us and presenting us with ever more adversity and ever more limited policy options. Throughout this report, we highlight specific recommendations that the Subcommittee has acted on or intends to address in the future.

II. The Cost of Failure

Einstein's letter to President Roosevelt warned of an unimaginably powerful bomb in the hands of Nazi Germany. Today, the Pentagon takes seriously the threat of game-changing weaponry in the hands of our adversaries and the IC appreciates the threat of falling behind in surveillance, data management and cryptography. The prospect of hypersonic weapons, bio-altered "super soldiers," or swarms of autonomous drones keeps national security leaders up at night. But it is important to remember that less Hollywood-esque advances in more obscure technology, and indeed in esoteric processes, procedures and culture, may pose a greater threat to our national security.

In considering the risks associated with technological innovation, it is critical to consider not just linear progress in the development of the outputs (the aforementioned weapons and drones) but the overall health of the inputs: that is, the people, funding and environment in which they come together to produce innovation. Getting the inputs wrong will, over time, assure the failure of the outputs. There is a tendency in the broad policy community to focus on those outputs. Technology is usually tangible and sometimes captivating. There is a reason why "Q" is a critical part of every James Bond movie. Since World War II, the U.S. has also generally held a meaningful qualitative edge over its adversaries in technology. So, it is not hard to conjure alarming scenarios around the deployment of "dual use" emerging technologies in the future:

- **Quantum computing** could help develop solutions to the world's most complex problems – from cures for cancer to climate change – because of its ability to run certain models and assess outcomes in a fraction of the time required by current computers. A scalable quantum computing capability could also defeat the toughest encryption, rendering unsafe U.S. nuclear command and control and the most secret communications of the United States government.[9]

- **Artificial intelligence** could alleviate the burden of some of humankind's most challenging tasks, by automating dangerous jobs, eliminating human error from medical emergencies, or predicting the weather.[10] In the future, AI could also be used to deploy thousands of autonomous micro drones for persistent surveillance or kinetic attacks against which defense would be nearly impossible.[11]

- Advances in **biotechnology** are creating ways to manipulate the very building blocks of life and could be used to address challenges from pandemics to world hunger.[12] At the same time, they might be used to develop weapons that target specific human genotypes.[13]

Failing to lead the world in any one of these technologies might reset the international order, threaten the norms that have guided international conflict and competition, and undermine the model of international cooperation and leadership that has existed since the end of World War II. However, ambush by game-changing technology is not the only concern: incremental technological advances can also threaten economic and national security, as the Chinese telecommunications firm Huawei's commercialization of fifth generation cellular technology ("5G") has shown.[14] Huawei is the world's largest provider of telecommunications equipment and has been steadily growing its market share.[15] Its main competition comes from the Swedish company Ericsson and the Finnish company Nokia, which struggle to match the price and performance of Huawei's offerings.[16]

5G networks will offer lower latency, higher bandwidth, and the capacity to interconnect our lives into the "internet of things." It will also generate vast quantities of personal and commercial data for those enabling (or with access to) such networks.[17] In its 2012 investigative report on the Huawei and ZTE, this Committee noted that with Chinese equipment in telecommunications networks, "the opportunity exists for further economic and foreign espionage by a foreign nation-state already known to be a major perpetrator of cyber espionage."[18]

The risks of losing the technological race to the outputs are tangible in a way that decay and erosion in the critical inputs of innovation are not. When Q appears in a James Bond movie, we see his toys, never his budget, the quality of his staff or the attitude of his overseers. Though evident on a graph, the declining U.S. market share in basic global research will never be the core theme of a Hollywood thriller. When top-notch programmers leave the National Security Agency ("NSA") for the private sector, when layers of oversight or politics punish risk taking or creativity, few notice. However, money, people, culture, processes and incentives matter tremendously. And the Subcommittee believes that in this area of innovative inputs, the reviews are decidedly mixed.

Today's intelligence and military industrial base has evolved dramatically since World War II and is characterized by many layers of bureaucracy, extensive oversight and review, consolidating contractors, lengthy development cycles, and most unsettling of all from the standpoint of innovation, intolerance of risk. These attributes usually developed for sound reasons. But their effect today, particularly in the all-important realm of software and its rapid and agile development, can be deadly.

Christian Brose, former Staff Director of the Senate Armed Services Committee, in his book *The Kill Chain: Defending America in the Future of High-Tech Warfare*, explains the evolution in stark terms:

> "Eisenhower had directed the military-industrial complex to incredible effect, whatever misgivings he ultimately developed about it. But somewhere along the way, Washington turned against Eisenhower's risk-tolerant approach that had enabled innovators such as [General Bernard] Schriever and others to do the impossible, and then spent decades replacing it with cumbersome, stultifying central planning processes that could not deliver great technology fast or at all. Washington sacrificed speed and effectiveness in the military-industrial complex for the hope of cost savings and efficiency, and it ended up with neither. It is as if America defeated the Soviet Union and then went about adopting the Soviets' military procurement system."[19]

The risk that Brose describes, which has been highlighted by many leaders such as former Secretary of Defense Ashton Carter, the Defense Innovation Board ("DIB"), its first chairman, Eric Schmidt, General John Hyten and Dr. Will Roper, is immensely complicated, touching on culture, incentives, congressional turf and political concerns, among many other factors. The challenges of achieving speed, agility, accountability for the end user and acceptable levels of risk affect nearly every piece of technology and every aspect of innovation inside the IC.

Nowhere are the risks of failure and the rewards for success more dramatic than in the realm of software and its development. Software, which is all too often thought of as just another product to be acquired or developed, is anything but. Yes, it is an output of innovation, but the environment in which it is developed—its speed, agility, responsiveness to the end user and constant real time improvement—is an essential input to almost all innovation.

Marc Andreessen, an iconic technology investor, famously noted in a 2011 article that "software is eating the world".[20] He meant that every aspect of life, including national defense, has become deeply entangled in and dependent on software. It is only a small exaggeration to say that software has eaten just about everything in the IC.

The core activity of the IC is the collection, analysis and storage of vast quantities of information: images and electronic signals of nearly infinite varieties, voice data, thermal signatures…the list goes on and on. Only in the briefest and most specialized of moments – a conversation across a table in an African café, a human judgment made of a photographic image – is software not collecting, sorting, cataloging, labeling, clarifying or presenting the data. The more exotic possibilities of next generation technology—megabytes of data carried in the cells of a housefly, emotional intelligence in a machine—will be enabled and countered by software.

Consequently, rapid, iterative, end-user focused software development capability is essential to our competitive position and to our very security. As Brose starkly notes, however, throughout our national security apparatus, software development is none of those things. As the DIB's excellent and solutions-oriented report *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage* notes, "The current approach to software development is broken and is a leading source of risk...it takes too long, is too expensive and exposes warfighters to unacceptable risk by delaying their access to tools they need to ensure mission success."

This report cannot touch on every aspect of undertaking a new approach to software development. A variety of other reports and analyses have done so. Fortunately, many elements of the national security effort, such as the Air Force's Kessel Run (discussed below) are currently modeling success. Many of the recommendations which follow would create the environment and provide the people to help accelerate and broaden this effort. In the aggregate, the Subcommittee believes that they will help ensure that when U.S. policymakers confront today's emerging technologies face-to-face, they are in the driver's seat.

III. RECOMMENDATIONS

Recommendation 1: Get the Money Right

Expand the Federal Commitment to Basic Research

Studies of American innovative capacity almost universally highlight the declining commitment to government-sponsored basic research. As demonstrated in Appendix A, nearly all of the reports reviewed by the Subcommittee called for substantial increases in federal funding. In fact, while the absolute federal commitment to basic research has grown over time, its share relative to U.S. gross domestic product ("GDP") has declined substantially.[21] The CFR Task Force notes that federal investment in basic research has fallen from a peak of 1.9% of GDP in 1964 to a level of 0.7% in 2016 and recommends a restoration of that funding to its historical average of 1.1%.[22] Many observers note that the private sector commitment to basic research, while growing meaningfully, will not necessarily be directed at government research priorities, but instead at developing commercial applications.

Perhaps of greater concern is the decline in all federally sponsored R&D relative to other countries. As Chart 1 illustrates, China is approaching and will soon exceed the U.S. share of global R&D investment if present trends continue. In this regard, China is a competitor in a different class from other U.S. adversaries such as Russia, Iran and North Korea.

Chart 1: Share of Global R&D of United States and China, 2000-2018[23]

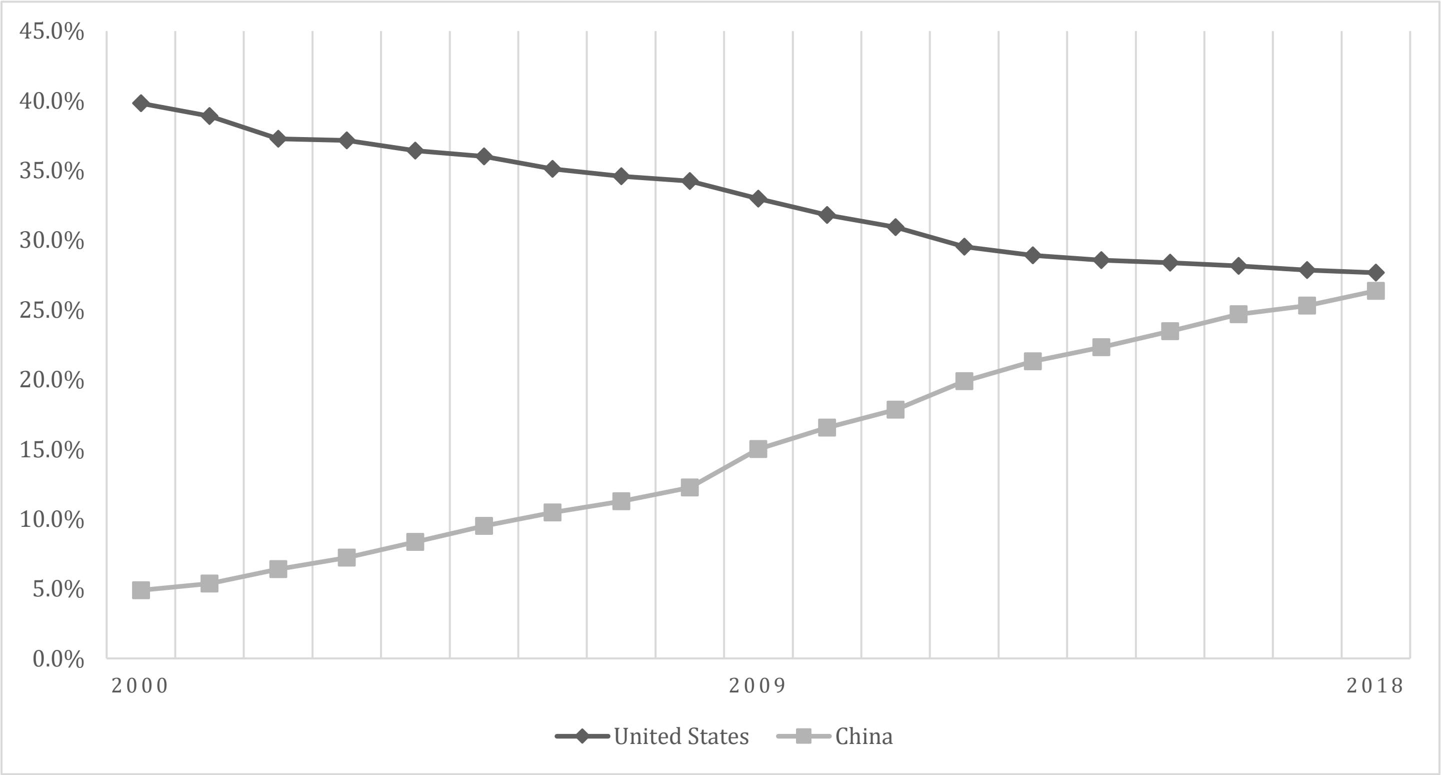
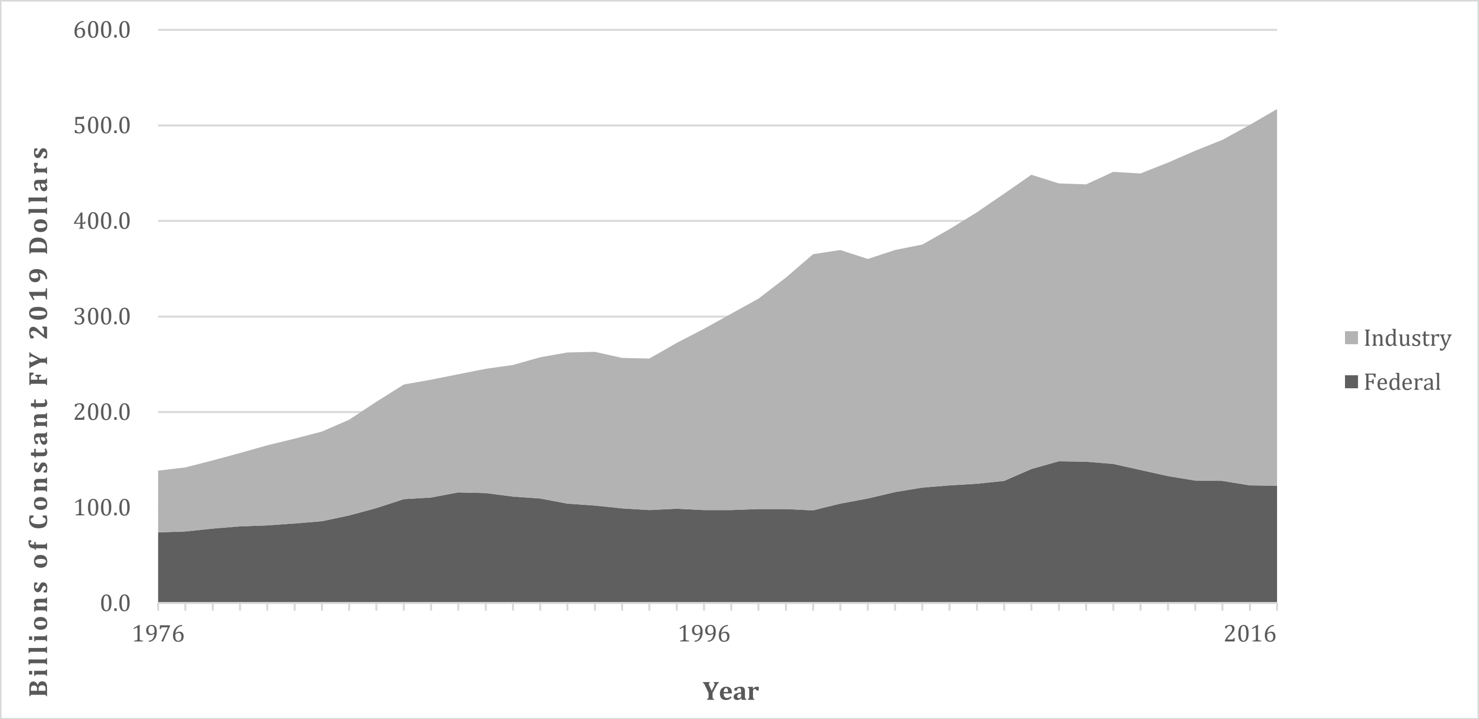


Chart 2: United States Federal Share in R&D, 1976-2017[24]



Quantifiable R&D expenditure may also understate the extent to which an adversary is financially committed to acquiring (as opposed to developing) intellectual property. Foreign direct investment ("FDI") into early stage companies has been of great interest to Chinese investors, some with clear links to the Chinese government. While overall Chinese FDI has fallen in recent years – from $8 billion per quarter in 2016-2017 to less than $2 billion in 2019 – venture capital investments grew to a record $4.1 billion in 2018, far outpacing the previous record of $2.6 billion set in 2015.[25] While China's $4.1 billion in venture capital investment is a small portion of total venture capital raised in the United States, it has been concentrated in a few strategic technologies.

While the Subcommittee believes that recommendations for increased federal spending on basic R&D are almost certainly directionally correct, we cannot ignore the changes in the global basic research ecosystem revealed by these trends. Increased federal funding alone will not be enough: it must be coupled with changes to how the IC organizes, establishes relationships, and sets priorities for R&D in order to be successful.

Recalibrate Spending on R&D

In addition to increased funding, the Subcommittee heard repeatedly that the current structure of the federal budget as it relates to innovation in the IC and national security generally is rigid in ways that make difficult the agile and flexible pursuit of ideas of uncertain success. This is particularly true when investing in any technologies that change rapidly to suit evolving requirements – often more frequently than can be accommodated by an annual budget and appropriations process – and for which the line between acquisition and maintenance is not, and in fact should not, be clear. Unfortunately for our government, many of today's most relevant and cutting-edge technologies – from software to biotechnology – fall in such a category.

The appropriations process is – for good reason – designed to buttress Congress' power of the purse. Appropriations are for specific amounts of money, allocated for specific periods of time, usually attached to some framework of milestones designed to provide congressional committees with plentiful opportunities for oversight. The committees of jurisdiction have ever changing membership, and those members offer uneven (some might say quirky) levels of focus over time. Combined with the frequency of continuing resolutions and shutdowns in recent years, these factors work against the unique combination of predictability, sustainability, and flexibility that optimizes the production of valuable research. As the *Software is Never Done* report observed, “Congress and DoD have created a massive body of laws and regulations that are just slowing things down…[and] should focus on rewriting selected pieces of old code (=legislation and regulations) that are doing more harm than good.”

The Subcommittee intends to pursue a number of the changes proposed in the DIB’s report, including a) new acquisition pathways for software; b) the creation of a software appropriations category that combines R&D, production and maintenance into a single budget item; and c) the deployment of empowered digital experts throughout the IC to assist and promote the rapid and iterative deployment of software to the end user. The Subcommittee will also consider further ways to reduce the uncertainty injected into research projects by the often short-term quality of available money.

Recommendation 2: Get the People Right

Venture capital investors, whose livelihood depends on identifying successful innovation, often focus on finding and supporting *innovators*, that is, people. The IC is and must continue to strive to make itself an attractive destination for the talent it needs. This involves bridging disparities in both pay and culture relative to the private sector. The IC will likely never match the speed or flexibility of private sector hiring, nor can it compete with its pay, particularly in critical areas like cybersecurity and AI.[26] It should, however, leverage its unique attributes: a distinct national mission suffused with pride and patriotism and the opportunity to work with technology and people not available outside of government.

Broaden Targeted Hiring Authorities

Compensation issues should not be ignored entirely, and in fact, there exist mechanisms to reduce the compensation gap. In 2017, Congress authorized the head of each element of the IC to establish higher minimum rates of pay for positions that require expertise in STEM.[27] The NSA was granted authority to establish a special rate of pay for positions that perform cyber-related functions.[28] In addition to those IC-specific mechanisms, the IC can utilize government-wide authorities to hire experts on a temporary basis, referred to as “special government employees” (“SGE”) or “highly qualified experts” (“HQE”). The SGE authority allows agencies to appoint temporary, part-time employees outside the standard hiring process.[29] The HQE authority permits government agencies to offer higher pay and more flexible onboarding processes for people with relevant qualifications.[30] Besides compensation, the federal government, beginning October 1, 2020, will grant up to 12 weeks of paid parental leave to all federal employees following the birth, adoption, or foster of a new child – a benefit rarely offered in the private sector.[31]

Elements of DOD, such as the Defense Advanced Research Projects Agency (“DARPA”), have benefited from special hiring authorities to fill technical positions through an expedited hiring process and increased pay, enabling them to attract top-tier talent.[32] The Intelligence Advanced Research Projects Activity (“IARPA”), an office within the Office of the Director of National Intelligence (“ODNI”) with a similar mission of advancing basic research, might benefit from similar hiring authorities, as would other IC elements. These positions offer preeminent experts an opportunity to spend a defined period leading government research efforts and advising major agency initiatives. The term-limited nature of these positions helps ensure that these personnel do not compete with government employees for promotion. While attracting the right talent is essential, new hiring authorities are not a silver bullet.

The Subcommittee believes that the IC's existing hiring authorities are underutilized, but that more information is needed before undertaking legislative changes. Therefore, we recommend that ODNI conduct a study to determine whether existing authorities fail to fulfill the IC's need for highly skilled STEM talent, and whether a companion authority similar to that given to DARPA would fill such a gap.

Expand Retention Incentives, Including Student Loan Repayment Plans

IC employees – like other federal government employees – can qualify for the Federal Public Service Loan Forgiveness Program if they remain in public service for 10 years and make on-time payments on their student loans throughout that period. Some federal agencies also provide financial contributions to their employees in exchange for a commitment to remain employed for a period of time.[33] The IC's record here is not uniform, with some elements or their parent agencies offering repayment assistance for certain categories of personnel and others not offering assistance whatsoever.

The federal government should offer such support to all federal employees, but in the absence of such a policy, we recommend that all IC elements establish support for federal student loan payments and, as noted in the FY 2021 IAA, consistent standards for federal student loan repayment eligibility.

Create a STEM Fellowship Program in the IC

IC policies should be updated to reflect the fact that many graduates and mid-career professionals may not be interested in a lengthy career in the federal government.[34] STEM professionals have strong incentives to change jobs frequently in order to expand their skill sets and stay current on cutting-edge technology development.[35] The IC's recruitment, security, and onboarding processes were designed in a time when the goal was to recruit and retain career personnel, and thus the process often overlooks those with the right skills who would be interested in a shorter period of service.[36]

The Presidential Management Fellowship offers a constructive model for shoring up the IC's STEM workforce. We recommend that the IC explore the creation of a technology fellowship program similar to the Presidential Management Fellowship oriented towards recent STEM graduates.

Engage with Educators

The Subcommittee believes that the IC should broaden its engagement with academic institutions at every level; not just to undertake immediately valuable research, but to help encourage the STEM pipeline and better cultivate future recruits. Colleges and universities are necessary partners, and not merely because they are educating the future IC workforce. Engaging with K-12 students must continue to be a component in the IC's STEM recruitment strategy. IC elements that are part of the DOD have statutory authority to establish educational partnerships and to ensure such institutions are preparing their students for careers with the federal government, which is of particular importance when the skills are in the highly-coveted STEM fields.[37] These relationships also facilitate information sharing. Over the course of the Subcommittee's survey, the Central Intelligence Agency ("CIA") sought additional authorities to empower it to establish relationships with academic institutions in the same way as DOD IC elements do.[38]

Photo: Massachusetts Institute of Technology

The Subcommittee supports this request in the FY 2021 Intelligence Authorization Act, and also recommends the ODNI produce a report identifying gaps in how the IC governs its relationships with academic institutions with the *goal of informing further legislative changes (as necessary) in the FY2022 Intelligence Authorization Act.*

Explore Talent Exchanges

Another area to spur a more constructive dialogue between the IC and the private sector is for each to spend some time walking in the other's shoes. A public-private talent exchange would expose IC personnel to the practices and culture of the private sector and affirm the existence of extensive legal and policy restrictions over IC operations to public skeptics. More fundamentally, each would gain first-hand exposure to the contributions of the other.

In the FY 2020 Intelligence Authorization Act, Congress required the Director of National Intelligence to develop policies, processes and procedures to facilitate the detail of IC personnel to the private sector, and vice versa.

Accelerate Security Clearance Reform

The Subcommittee's review encountered frequent frustration at the cumbersome, time-consuming, and backlog-laden security clearance process. Until recently, the average security clearance would take two years to be completed, with certain candidates waiting as long as five years. At a time when national security threats change and evolve in weeks and months, that is not acceptable, particularly in the context of numerous recent high-profile breaches and unauthorized disclosures of highly classified information.

As a consequence, renewed attention to the security clearance process in the last several years has led to significant process changes. Notably, the government is transitioning to a "continuous evaluation, continuous vetting" model, which requires an *ongoing* reevaluation of personnel with security clearances rather than the "periodic reinvestigation" approach. In addition, the government is transitioning all government background investigations to DOD's Defense Counterintelligence and Security Agency from the Office of Personnel Management.[39] Federal agencies with the authority to adjudicate clearances are also working to synthesize and develop government-wide standards and reciprocity for personnel moving from one agency to another.

Recent progress has been made in reducing the backlog, from its peak of over 725,000 open investigations to 205,000 in July 2020, and in average processing time for Top Secret clearances, which has been cut by more than half, from 411 days to 79 days.[40] Such improvements must be sustained while the interagency council develops government-wide standards as well as reciprocity protocols to ease the bureaucratic burden on agencies and personnel seeking security clearances.

Reconsider Whether All IC Personnel Require a Security Clearance

Security clearance processing times stretching into years slow progress and dissuade many highly qualified applicants from embarking on a career in the IC, including many with STEM backgrounds.[41] Providing opportunities for STEM-oriented recruits to begin work before receiving their clearances would allow the IC to retain more candidates throughout the clearance process. Opportunities exist for open source intelligence work, training and coursework, research collaborations with academia and industry, and building capabilities that can be developed outside a secure facility.[42] This could be particularly beneficial for the STEM workforce: unclassified research partnerships, such as with the Laboratories for Physical Science and Telecommunication Science housed at the University of Maryland[43] offer opportunities that could be expanded to allow STEM recruits without a security clearance to contribute to the IC's mission.

The COVID-19 health crisis has prompted sweeping changes in the way people work, including IC personnel; the impact of the pandemic on the IC's work is particularly dramatic since nearly all work performed by the IC is done in secure facilities.

The Subcommittee believes that a Top Secret clearance is not necessary for all IC personnel to perform their job responsibilities, and for S&T R&D in particular, much work can be completed without even a Secret-level security clearance.

We recommend that the IC use its experience with COVID-19 to produce a report to Congress identifying IC positions that require personnel to maintain security clearances and at what level, IC activities that can be performed outside of secure facilities, and for those personnel who do require a security clearance, what authorities or policy restrictions might prevent the IC from placing new employees in positions lacking the clearance requirement while they wait for their security clearance to be complete.

Fix Immigration to Get and Keep Talent

Scholars of innovation have repeatedly pointed out the importance of skilled immigration to innovation in the United States and abroad.[44] Israel's small but highly innovative economy has benefited from mass high-skilled immigration,[45] and CSET notes that other countries, including Canada, are modifying their immigration systems to lure talent away from centers of technological innovation – including the United States.[46] The National Science Foundation describes the situation bluntly:

> Foreign-born workers—ranging from long-term U.S. residents with strong roots in the United States to more recent immigrants—account for 30% of workers in [science and engineering] occupations. The number and proportion of the [science and engineering] workforce that are foreign born has grown. In many of the broad [science and engineering] occupational categories, the higher the degree level, the greater the proportion of the workforce who are foreign born. More than one-half of doctorate holders in engineering and in computer science and mathematics occupations are foreign born. In comparison, about 18% of the overall population and 17% of the college graduate population in the United States are foreign born.[47]

This is particularly problematic for the IC, which has rigorous vetting procedures for its personnel,[48] including the requirement that a person seeking a job be a U.S. citizen.[49] If the United States is serious about maintaining its edge in science and technology, it must tap the highly-qualified foreign-born students that U.S. academic institutions are educating.

In order to leverage this largely untapped resource, the United States must grapple with its onerous, bureaucratic, and backlogged immigration system.[50] A flexible immigration system – particularly to facilitate access to highly-skilled scientists and engineers – is essential to innovation and the STEM workforce in the United States.[51] The national debate on immigration is currently generating far more heat than light, and a comprehensive solution to this issue extends well beyond the jurisdiction of this Subcommittee, but we cannot ignore the calls from across the political spectrum for meaningful reform, nor can we overlook the benefits that would accrue to the national security of the United States.

Recommendation 3: Get the Environment Right

Adequate resources and creative, empowered people are necessary, but not sufficient, conditions for innovation. Environment, which is less tangible and quantifiable than money or the talents of people, is also essential. Were it not, American innovation, rather than being highly concentrated in a few locations like Silicon Valley, Boston, New York and Austin, would be significantly more evenly distributed.

What makes for an innovative environment is subject to debate, but a variety of essential qualities are obvious: an open, collaborative culture, often between innovators and nearby academic and research institutions; a culture which embraces, rather than punishes risk-taking; an almost religious devotion to doing things differently—what economists call "disruption" and what Mark Zuckerberg called "breaking things". These are not qualities that are readily embraced by the federal national security apparatus. The Subcommittee offers several ideas to improve the status quo, ideas which are largely about collaboration. As Steven Johnson, author and student of innovation notes, "If you look at history, innovation doesn't come just from giving people incentives; it comes from creating environments where their ideas can connect."

Invest in Private Sector Partnerships

The dramatically increased share of private investment in R&D makes clear the need for close partnership between the government and the private sector. The dramatic array of products and services emerging from private industry have more relevance than ever before for the IC, particularly in AI. But quicker access to products is not everything; knowledge sharing, constructive relationships with people and trust are essential to national security.

Some national security leaders believe that in areas such as AI and biosynthesis, private firms are ahead of the government in innovation.[52] Sue Gordon, former Principal Deputy Director of National Intelligence ("PDDNI"), has suggested that for certain technological innovations, the government should seek not to lead in innovation, but to be a "fast follower".[53] In a competitive context in which adversaries like China are moving fast, the United States should, at the very least, seek to be not just a fast follower, but the *fastest* follower. But the IC cannot assume that private industry will share products, ideas and research openly with government by default. For the government to keep abreast of and benefit from these innovations, it must be a partner and a customer.

Suspicion and tension between the private sector and the government has, particularly in the last decade, impeded the trust and relationships required for a healthy innovation ecosystem. Concerns about how the U.S. government – and the IC specifically – respects privacy rights; how foreign adversaries have manipulated technology platforms to interfere in politics; and unauthorized disclosures revealing to the public the breadth of information being turned over to the government by the private sector have all exacerbated distrust.[54]

Apple's refusal to assist the Federal Bureau of Investigation ("FBI") in unlocking the iPhone belonging to the deceased terrorist who carried out the 2015 San Bernardino terror attacks created concern in the minds of many national security professionals. Shortly after, Twitter instructed Dataminr – a company in which Twitter held a 5% stake – to cease a pilot data-sharing program with the IC, in which the IC was receiving Dataminr's curated, algorithm-driven feeds of public Twitter posts.[55] The protest mounted by thousands of Google employees against their company's participation in DOD's Project Maven in 2018 resulting in the withdrawal of Google from the project and from its work to run the DOD's Joint Enterprise Defense Infrastructure cloud computing effort also raised concerns.[56] It was not lost on many national security professionals that Google continues to assist foreign countries, such as China, with their technological development.

In order to reduce tension and build trust, the IC must speak more openly and publicly about its mission, values and challenges. IC leaders must be more accessible and public-facing. The NSA's former Director of Research, Dr. Deborah Frincke, for example, made a priority of speaking publicly about NSA's research mission when she took the helm of the Research Directorate.[57] Given the stakes, her approach involved risk, required care, and undoubtedly raised eyebrows. But she succeeded, and her speeches – memorialized on YouTube and elsewhere – are persuasive arguments for the IC's mission that will pay dividends in the long-run.

Another prominent confidence building measure that has improved the tenor of the IC-private sector relationship is the Vulnerabilities Equities Process (the "VEP"). The VEP is an interagency process that weighs the public interest for the disclosure of a cybersecurity vulnerability identified by the U.S. national security community. Although its proceedings are classified, the White House has spoken publicly about the VEP, and there is open dialogue between the VEP membership and Congress about its work. The VEP has streamlined communication between government and industry by providing a framework for the government to deliberate and ultimately provide a coherent, united assessment on cyber vulnerabilities to the private sector and the public.[58] Notably, its resulted in the disclosure to Microsoft of a highly problematic bug in its operating system that undermined the reliability of the software's certification. In layman's terms, without the patch, hackers could spoof a user's certificate to trick the operating system to grant the hackers access to the system. Microsoft released a patch in January of 2020 and attributed its discovery to NSA.[59]

When she was PDDNI, Sue Gordon often spoke about the need for more interaction between the IC and the private sector, and promoted the concept of a public-private partnership to address shared challenges, such as how to apply an ethical framework to the use of AI. Gordon has frequently argued that IC leaders should seek opportunities to act as ambassadors to the private sector.[60]

The Subcommittee believes that IC leaders should be more recognizable to the public, but that they must also establish personal relationships with industry and academic leaders. IC leaders deliver speeches at events like RSA, Black Hat, and the Aspen Ideas Festival, and interact with other prominent leaders on the margins of those events.[61] These engagements serve an important purpose from a public relations perspective, but trust and relationships grow deeper in private settings. The IC and private industry and academia will not – and should not – agree on all of the complicated issues surrounding the IC's work, but building relationships of trust is still important. Unlike other government officials who may come in from the private sector at senior levels, many current IC leaders have spent decades in military or civilian federal service, with few opportunities to develop strong networks outside of government circles.[62]

Strengthening personal relationships will catalyze information sharing, problem solving, and collaboration. We recommend that, in a manner that is consistent with federal ethics and contracting laws, the top three officials at *each IC element take at least one private meeting a month with industry and academic leaders.*

The IC should also consider how to better leverage the remarkable In-Q-Tel model. In-Q-Tel is an IC-funded non-profit established to identify and enable technology startups and facilitate ready-soon technology adoption for national security purposes.[63] In-Q-Tel's extensive relationships in the venture capital and technology communities provide it a unique perspective into trends in cutting-edge technologies and the ability to translate between the operational requirements of the IC, the technical expertise of a startup, and the investment language of venture capital.[64]

In-Q-Tel also delivers technologies to the IC at great value to taxpayers. Each dollar of taxpayer funds invested by In-Q-Tel in technology startups leverages an average $16 of private venture capital. While the investments it makes are small relative to the investment from traditional venture capital firms, its investment dollars are a signal to others of a company's viability.[65] Furthermore, nearly 70% of investments made by In-Q-Tel result in field-tested capabilities by IC customers.[66]

We recommend that the IC identify ways to leverage In-Q-Tel's unique position and connections with innovators outside the traditional Defense Industrial Base to broaden the pool of partners the IC can utilize to accomplish its missions. We also recommend that the IC assess whether (or how) to leverage In-Q-Tel's visibility into tech startups and the investment community for broader situational awareness of domestic and foreign technology trends.

Learn Software Development Fast

The history of the national security establishment, and of DOD in particular, of building and acquiring software over budget and behind schedule is a worrying case study for how legacy government processes can impede innovation.[67] It has long been considered industry best practice to develop software in an "agile" way, developing and releasing features in small iterations and then incorporating user feedback into future iterations.[68] DOD seems to have too often failed to follow this and other best practices, running the risk that vulnerabilities remain unpatched and the software is outdated by the time it is deployed.[69] As far back as 1987, the Defense Science Board noted the importance of these practices as well as the DoD's resistance to using them.[70] In its 2019 Software Acquisition and Practices Report, the DIB noted that remarkably little had changed in the intervening 30 years.[71]

For DOD, the result of this inaction has been numerous software programs that are delayed or over budget, and in some cases cancelled outright.[72] While culture and inertia play a role, it is clear from the DIB's work that structural limitations prevent DOD from innovating at the speed of mission. In addition to creating security risks, outdated software practices threaten the IC's ability to manage its exponentially increasing quantities of data and its ability to develop automation and artificial intelligence.[73]

The Subcommittee believes that these challenges exist in the IC, but to a lesser extent, since the IC, and particularly NSA, has always relied extensively on software and its rapid creation and deployment, as well as considering itself its own systems integrator. It is clear that different IC elements are evolving to private industry's "DevSecOps" approach at different rates, so the Subcommittee urges renewed focus on this critical change and on models for success.

One of the more remarkable models of software development success is Kessel Run. In 2017, the Air Force established Kessel Run as an experimental program to enlist software engineers, designers, and product managers from San Francisco-based Pivotal, Inc. to work collaboratively with Airmen and steep them in the practices of the technology sector.[74] The success of Kessel Run's model stems in large part from its willingness to challenge longstanding cultural norms in the DOD and to adopt best practices from the technology industry. Its extensive use of Direct-Hire Authority to expedite the hiring of engineers, designers, and others with the skills essential to drive software innovation is but one example.[75] Congress established this authority in 2002, but its growth has been slow and uneven, in part due to cultural resistance.[76]

Kessel Run shifted DOD information technology security processes to more closely align with industry best practices. By automating the process of testing its software for bugs and security issues, Kessel Run can update its software multiple times per day rather than in months-long cycles, improving both the value and security of its products.[77] The first project Kessel Run tackled saved the Air Force several million dollars per week for an estimated investment of just $2.2 million.[78] The Air Force and DOD are now replicating the success of Kessel Run as they establish new software factories.[79]

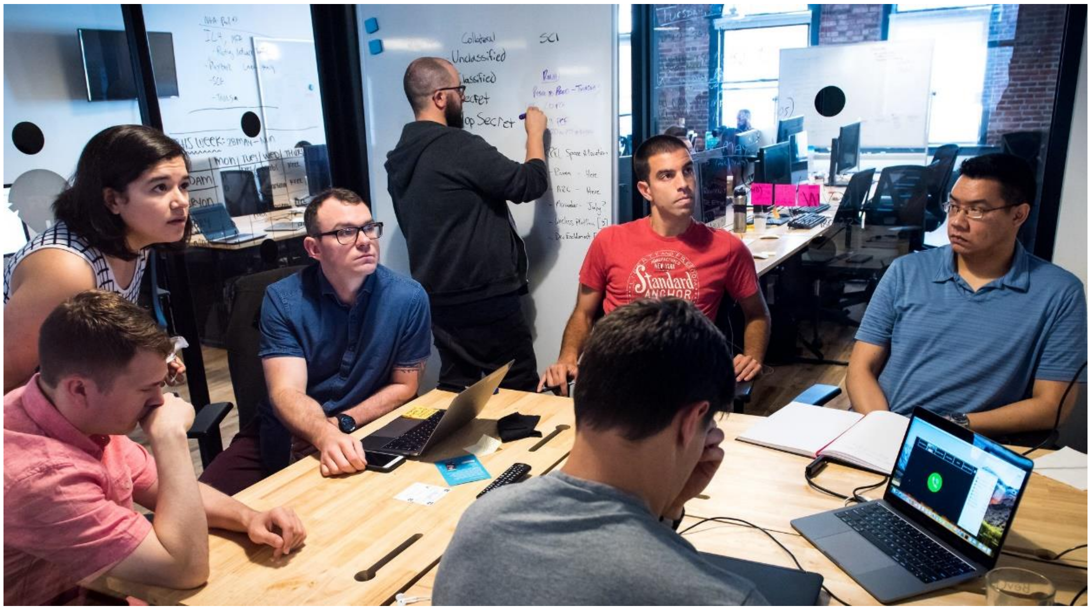


Photo: A software development team conducts an Iteration Planning Meeting about a software project in the office of Kessel Run. Photo credit: U.S. Air Force photo by J.M. Eddins Jr. Attribution-NonCommercial 2.0 Generic (CC BY-NC 2.0) Photo link. License link. Disclaimer: The authors of this article are not responsible for and do not endorse any content found on flickr.com or creativecommons.org. No changes made.

Those IC elements that struggle with software development are encouraged to seek out partnerships with the private sector to absorb best practices. While Kessel Run's model may not be a perfect match, IC elements should seek to adopt the best practices of DevSecOps in appropriate ways. Good software also requires good infrastructure. While the IC is a government leader in areas like cloud computing, it still faces challenges migrating legacy systems and data to the cloud, and continued work is necessary.[80]

In order to facilitate greater awareness of software best practices and provide incentives for their adoption, we recommend the IC explore creating a pilot to automatically track and report metrics on software programs' adherence to modern best practices.

Rethink Acquisition Procedures and Culture

The IC should strive for improved agility in areas beyond software development. It should rethink how it purchases other systems, goods, and services. In his testimony before the House Armed Services Committee in April of 2018, Dr. Eric Schmidt, the first Chairman of the DIB and former CEO of Google, opined that DOD "does not have an innovation problem; it has an innovation *adoption* problem."[81] Schmidt's insight was driven by his observation that the military has many entrepreneurial members, and a variety of innovative units (like Kessel Run), but that sclerotic processes, systems and incentive structures make it very hard for innovation to reach the warfighter. He identified acquisition and procurement as a brake on adoption.

The IC is not the Pentagon and does not undertake major systems acquisitions in the routine way the DOD does for aircraft carriers, submarines, and F-35 jets over generations-long acquisitions and procurement cycles. In fact, the Pentagon's FY20 procurement budget of some $140 billion was nearly double the entire budget of the IC the same year.[82] Nonetheless, acquisition and procurement are critical for the IC in today's technology-driven world, and therefore many of Dr. Schmidt's observations are also germane to the IC's acquisition of systems, goods, and services.

The barrier to entry for companies to work with the IC is particularly high – potential suppliers must understand a complex web of federal contracts, acquisitions processes, and export controls, and have the necessary infrastructure in place to provide its systems, goods, or services to its government customer.[83] They must also meet security and background check requirements, and, depending on the nature of the work product, have personnel with high-level security clearances.[84]

More versatile models that could help the IC work with nontraditional partners often go underutilized. For example, Other Transaction Authority ("OTA") – a flexible acquisition authority with origins in the space race – is often avoided because lawyers and acquisition officials are less unfamiliar with it relative to more traditional acquisition vehicles.[85]

In order to more fully understand how the IC is (or isn't) leveraging OTA, we recommend that the IC produce a report that examines the use of OTA by IC elements on a yearly basis and provide that report to this Committee.

Invest in Open Source Intelligence

As the international community's tracking and analysis of the spread of COVID-19 has graphically demonstrated, intelligence collection must not be confined to traditional methods like secret meetings and technical means at Langley or Fort Meade. Historically, the IC's open source intelligence ("OSINT") mission was conducted by the Foreign Broadcast Information Service, which compiled and translated foreign broadcast reports relevant to the IC's mission. Many of these reports were subsequently made public, enriching the United States' collective understanding of the plans and intentions of our adversaries.

The evolution of the foreign media landscape, digitization of information, and worldwide connectivity is still under-appreciated in the IC as a key collection opportunity.

Over the years, IC OSINT capacity has been repeatedly reorganized, including the establishment and subsequent dissolution of the Open Source Center. This has raised questions about the overall level of priority placed upon its mission. Just as open source information can generate valuable intelligence about foreign cyber actors' intentions and activities against commercial and private networks, so too can open source provide the sort of lead information and context to drive the IC's S&T intelligence analysis. Analysis of investments in start-ups, the establishment of academic partnerships with top-notch researchers, and even scrutinizing the members of a social networking group contribute to the IC's assessments of adversary capabilities on S&T, which in turn will help counter those advances.

The Subcommittee sees a strong future for OSINT within the IC, so long as it receives the appropriate attention and resourcing. Coupled with AI and machine learning, there are exciting new possibilities for the development of open source intelligence programs.

Consequently, the Committee's FY21 IAA commissions an independent study on open source intelligence, to develop recommendations for the future governance of OSINT within the IC.

Leverage and Nurture the Federal Labs

The FFDRCs and the University Affiliated Research Centers ("UARCs") originated in the Manhattan Project and other federal R&D efforts during World War II.[86] The IC currently benefits from the talent of the Department of Energy ("DOE") National Laboratory FFRDCs under the umbrella of the Strategic Intelligence Partnership Program ("SIPP").[87] Although the SIPP enables DOE National Laboratory personnel to support unique, vital IC-sponsored research, the Subcommittee believes that there is insufficient strategic direction, which hinders the National Labs from fully addressing the hardest national security problems.

Photo credit: Sandia Lab photo by Randy Montoya. Attribution-NonCommercial-NoDerivs 2.0 Generic (CC BY-NC-ND 2.0) Photo link. License. Disclaimer: The authors of this article are not responsible for and do not endorse any content found on flickr.com or creativecommons.org. No changes made.

For example, while DOE's Office Intelligence and Counterintelligence ("DOE-IN") plays a centralizing function between the DOE National Laboratories and sponsoring elements from the IC, its responsibilities are, as a matter of staffing and practice, largely constrained to administrative processing of project submissions. The Subcommittee sees an opportunity for DOE-IN or another appropriate body to adopt a more assertive role in strategic coordination, deconfliction, administrative processing, and even technical advisement, to improve the alignment of IC needs with National Laboratory capabilities.

The Subcommittee also found that IC sponsors and their National Laboratory counterparts rely on professional relationships to develop prospective SIPP projects.[88] Although the Subcommittee views this avenue as beneficial, it believes that increased formality would help ensure that IC elements fully utilize the wealth of top-tier science and technology talent and capabilities available across the FFRDC community.

We recommend that Congress require DOE, DOD, and the IC to conduct a joint review of their respective roles in administration, oversight, coordination, and deconfliction to ensure the IC best leverages the expertise of the FFRDC and

UARC community. Such a review could also inform how the IC and the DOD access the wider federal lab community to tackle additional national security challenges.

Collaborate with Foreign Partners

The IC does and should continue to use foreign intelligence relationships as a force multiplier in developing emerging technologies. Many alliance and partnership frameworks exist to bring countries together. Most notably, the Five Eyes Alliance – the United States, United Kingdom, Australia, Canada, and New Zealand – was founded upon a shared mathematical endeavor to break German encryption. NATO was originally established to protect its Member States from further attacks by the Soviet Union after World War II. Since then, the IC has leveraged international relationships to achieve significant intelligence successes, and this cooperation should be expanded into greater scientific and technological R&D collaboration.[89]

Photo: NATO Headquarters, Belgium. Photo Credit: NATO

One indicative example is the NATO Innovation Hub, which provides both a virtual and physical platform for outside experts, who do not usually work with the defense and security community, to propose and design innovative technological solutions to some of NATO's most pressing security challenges such as human-machine teaming, autonomous systems, and cyber security.[90] Similarly, NATO recently created an Innovation Advisory Board of advisors and academics to help NATO “accelerate the pace of development and integration of unmanned systems in Allied and Partner navies.”[91]

Each of these collaborative frameworks share similar principles. First, they were “opt-in”; no state was required to participate, but the collaborative benefits enjoyed by those who did participate often brought in more participation. Second, these groups regarded technological innovation as not exclusively a national security issue, but also an economic one. Therefore, rather than limiting participation to individuals with national security backgrounds, the groups encouraged an array of perspectives. The Innovation Advisory Board is comprised not just of policymakers, but of academics and corporate executives in fields such as consumer products, defense, and technology.

International partnerships also allow countries to leverage their comparative advantages, as different countries often excel in specific and strategically important technology areas. Australia is a leader in quantum technology; Germany excels in additive manufacturing; Canada, France, Singapore, and Switzerland are home to some of the most advanced biotech firms in the world; and Israel, the United Kingdom, South Korea, and several Nordic countries excel in telecommunications infrastructure.[92] By working closely with these countries, and many others, the United States can build a coalition capable of leading global R&D. Only by working together can these long-time allies succeed, as CSET notes:

> America’s future lies in technical alliances. Taken together, the R&D spending of the United States and just six like-minded nations with a true commitment to R&D funding represents more than 50 percent of global R&D investment... China, on the other hand, makes up approximately 26 percent of global R&D, with other competitors like Russia contributing only two percent.[93]

We recommend that IC elements conduct comprehensive reviews of their foreign partnerships, and identify in a report to Congress specific areas ripe for further collaboration with foreign partners on scientific and technological R&D. The IC should also encourage programs that expand opportunities for collaboration with foreign partner governments, private industry, and academic institutions, such as through exchange programs and fellowships.

Congress, Heal Thyself

The Subcommittee would be remiss if we did not also acknowledge the role Congress has played in creating many of the barriers to technology adoption identified throughout this report. Amongst the many powers enumerated in Article I of the Constitution, two are particularly salient in this case – (1) Congress's "power of the purse" and (2) its stature as a co-equal branch of the U.S. government responsible as a "check and balance" on the Executive Branch. And the ways Congress has interpreted these powers – both in how it exercises them and in how Congress organizes itself – have created unique institutional challenges that impede innovation.

First, Congress jealously guards its "power of the purse" and is loath to cede any of its authority in this regard to the Executive Branch. Congress employs mechanisms that maximize its opportunities for oversight and management – some might say "micromanagement" – of Executive Branch spending of appropriated funds. These mechanisms range from limiting the availability of funds (some funds expire if not expended at the end of the fiscal year) to separating funds into different "colors" of money (e.g., funds authorized and appropriated for R&D may not be used to maintain or sustain a program). Combined with a rigid adherence to the annual budgeting and appropriations cycle, Congressional processes stymie the agility and flexibility needed to match dollars to the pace of rapid technological evolution.

Second, in executing its duty to oversee that the Executive Branch is a responsible steward of taxpayer dollars, Congress must ensure that departments and agencies are not taking unnecessary risks with those funds. As a result, Congress seeks to mitigate cost and program risk as much as possible and is rarely inclined to authorize or appropriate funding for programs that have uncertain time schedules and imprecise cost estimates. Program failures are often met with harsh penalties and very public rebukes from Congress which often fails to appreciate that not all failures are the same. Especially with cutting-edge research in technologies of the kind discussed in this report, early failures are a near certainty and, so long as they are not due to negligence, should be considered learning opportunities. In fact, failing fast and adapting quickly is a critical part of innovation.

Photo: United States Capitol

Lastly, Congress is not structured for cohesion or strategic unity. There is no single office responsible for ensuring that all the committees of jurisdiction for the various departments and agencies of the federal government are consistent in their funding approaches to emerging technologies, even though these technologies impact every single aspect of American life. Such a disparate approach means that often, committees spend more time adjudicating *who* has jurisdiction over a problem rather than *how* to actually solve the problem.

Congress should address these issues through existing, but underutilized mechanisms. For example, Congress has explicitly provided the Executive Branch multi-year “transfer funds” to address emergent and unpredictable requirements, such as natural disasters. These funds are large enough to ensure predictable and sustainable funding over time, and flexible enough that departments and agencies can draw upon them to address rapidly changing requirements outside of the annual budgeting and appropriations process. Because these types of funds are inherently flexible, they have been subject to mismanagement by departments and agencies; Congress sometimes derides these as “slush funds.” This problem should be solvable through the imposition of stringent notification and approval requirements on the use of these types of funds to mitigate the risk of abuse.

Finally, Congress would be a much better partner in innovation if its overall level of technical literacy were higher. Cutting edge technology, and the way in which it is developed, is often exotic to lawmakers. To address this, and to help break jurisdictional barriers, Congress should consider reviving the Office of Technology Assessment, which provided Congressional Members and committees with objective and authoritative assessments and analyses of complex scientific and technical issues. The Office was shuttered in 1995.

Recommendation 4: Improve IC Strategy and Vision

The Subcommittee's many discussions with IC elements surfaced satisfaction with the flow of S&T personnel across those elements and general agreement that the IC has made real progress against the stove-piping of innovative efforts across its 17 elements. However, the Subcommittee believes that while there may be some nominal level of oversight at ODNI over the entire IC R&D portfolio, there is a gap in the alignment of strategic thought leadership and prioritization of R&D activities in the overall IC. Rather than a single voice conveying the IC's priorities to policymakers and lawmakers, each IC element advocates for its own needs which can be niche or tactical in nature. Such strategic leadership is needed to ensure that the most critical programs receive the resources they need, and that the urgent does not win over the important.[94]

Focus IC Strategic Leadership

At present, the Director of Science and Technology of the ODNI, along with a nominal coordinating body, the National Intelligence Science and Technology Committee – established by Congress in 2004 – is tasked with overseeing the IC's scientific R&D portfolio.[95] Additionally, there is a body at the National Intelligence Council responsible for coordinating intelligence analysis on adversarial scientific research endeavors.[96] However, neither appear to have sufficient authority or resources to accomplish their rapidly growing missions.[97]

The Subcommittee also believes that a full appreciation of our adversaries' S&T activities is critical to success, and thus the ODNI's Director of Science and Technology should play an advisory role in the IC's analytic work on adversarial achievements. Finally, we acknowledge that additional layers of bureaucracy on S&T R&D could have the unintended effect of stymieing innovation, and thus our recommendations are modulated to create a clear line of strategic leadership on S&T, while leaving unchanged the organizations that conduct R&D.

Consistent with legislation in the FY 2021 IAA, we recommend that Congress strengthen the authorities of the DNI's Director of Science and Technology and the National Intelligence Science and Technology Committee, and require annual reports to Congress containing both the IC's strategy and priorities for scientific R&D as well as assessments of adversaries' scientific R&D

activities. Such information will aid policymakers and Congress in funding, authorizing, and enabling the advancement of this critical mission.

Establish an Intelligence Innovation Board

Successful catalysts of innovation in DOD offer useful lessons for the IC. As with the IC, significant cultural rifts exist between the DOD and private sector.[98] The DIB, conceived by then-Secretary of Defense Ashton Carter in 2016, exposes senior industry and academic leaders to DOD challenges, and applies its outside expertise to help craft the DOD's emerging technology strategies and initiatives.[99] The DIB's notable successes in this area include the creation of the Joint Artificial Intelligence Center and the DIB Software Acquisition and Practices study which meaningfully improved DOD's software development and acquisition.[100] The DIB has also addressed tensions between the private sector and DOD through initiatives like its AI ethics principles, which have now been formally adopted by the DOD.[101]

An Intelligence Innovation Board, modeled after the DIB, could bridge similar gaps for the IC. It could also identify best practices from industry and academia and recommend how to adapt these to the constraints imposed by the IC's missions. A dedicated board will allow its members to build the expertise and connections necessary to provide tailored and actionable recommendations to unique IC problems.

Therefore, the Subcommittee recommends the IC establish an Intelligence Innovation Board to bring fresh thinking to the IC, identify ways to improve cooperation with the private sector and help the IC become a better partner and customer.

Recommendation 5: Lead in the Development of Norms and Standards

Framing the security challenge posed by innovation exclusively as a race to be "won" is a mistake. Technological races rarely stay won, and technology and knowledge disseminate. Sometimes this is to our advantage: the memory of Americans looking up from the comfort of their homes at Sputnik in October of 1957 is unpleasant but instructive, inasmuch as the United States quickly demonstrated its ability to be a fast follower and to ultimately pull ahead of the Soviet Union in space exploration.

Today, Huawei's commercial lead in 5G technology and a Chinese scientist's shocking genetic editing of human twins in 2018 are just two reminders that the United States is not in control of global technological research—we don't determine the participants or even the direction of many proverbial races.[102]

Fortunately, there is ample precedent for the United States and the world to agree on rules, ethics and international structures that seek to regulate the development, use and spread of dangerous technology. From the development of the Treaty on Non-Proliferation of Nuclear Weapons in 1968 to the Geneva Conventions of the early 20th century, to the many centuries of the elaboration of concepts of "just war" and the laws of armed conflict, there is a rich tradition of friends and foe alike cooperating on mutually beneficial norms.

Prudence and morality alike dictate that the United States must lead not only in the research, acquisition, and employment of emerging technologies but also in the development of standards and norms for their ethical use. Energetic U.S. commitment to a rules-based liberal order is not only necessary for countering alternative frameworks favored by oppressive regimes: it will also provide a competitive advantage for democracies and open societies, which thrive in an environment of transparency, rule of law, and institutionalized fairness.

The cyber realm offers the most comprehensive example of the world trying to come to terms with previously unknown risks and challenges. Capabilities that were once available only to sophisticated actors are now readily available to anyone with a smart phone and an internet connection. While some cyber intrusions have targeted the U.S. federal government and

U.S. elections, such as Moscow's digital assault on the 2016 U.S. election or China's hack of the Office of Personnel Management, many others have targeted a wide variety of non-government entities.[103] These events include attacks on private companies like Marriott, Target, Capital One, and Quest Diagnostics, as well as unrelenting identity theft and ransomware attacks on private citizens.[104] Because cyberattacks currently transcend the usual bounds of national security to threaten almost all aspects of modern life, the United States must create and promulgate globally accepted norms in the emerging technology arena.

In fact, there have been efforts for years to establish basic "rules of the road," beginning most notably with the Tallinn Manual and extending through the recommendations of the recently released report from the United States Cyberspace Solarium Commission ("CSC") this year.[105] For years, the United Nations ("UN") has advanced multilateral discussions around the need for established cyber norms and principles. In 2018, the UN established its latest Group of Governmental Experts ("GGE"). This GGE's scope — "Advancing responsible State behaviour in cyberspace in the context of international security" — explicitly builds on prior GGEs and is tasked to:

> …continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States…[106]

The GGE construct can be awkward, as demonstrated by its predecessor's failure in 2017 to adopt a consensus report after two years of work.[107] There is the additional complication in the parallel, if not overlapping, Open-Ended Working Group ("OEWG") – of which Russia was a key proponent – on developments in the field of Information and Communications Technology in the context of international security.[108] How the GGE and the OEWG will reconcile their efforts, and whether each group's findings will be at odds with the other's, remains to be seen. The United States' participation and leadership in such efforts, with key allies including the United Kingdom, France, Australia, and Canada, signals important commitment to proactively shape dialogue and progress.[109]

The realm of AI will also require substantial focus as technologies emerge and mature. AI poses ethical questions regarding inadvertent bias and auditability, as well as questions of human control and intervention. In response, several organizations have offered potential frameworks for the use of AI:

- ODNI has released both a Principles of AI Ethics for the IC as well as an IC AI Ethics Framework, which provides technical guidance for IC personnel to apply the Principles.[110]
- The DIB recently published its AI principles for DOD "for the design, development, and deployment of AI for both combat and non-combat purposes."[111]

The National Security Commission on Artificial Intelligence ("NSCAI") is also examining this issue, as noted in its interim report: "[t]here is an ethical imperative to accelerate the fielding of safe, reliable, and secure AI systems that can be demonstrated to protect the American people, minimize operational dangers to U.S. service members, and make warfare more discriminating…The American way of AI must reflect American values—including having the rule of law at its core." [112]

While the NSCAI's remit is limited to AI, we consider this conclusion broadly applicable to other areas of emerging technology: "The state or group of states that achieves technical leadership will have unique opportunities to set standards, build guard rails, and generate global support for what is acceptable and what is not in AI's future."[113] To accomplish this, the United States must exercise greater leadership and work more closely with its international partners. CSIS agrees: "The United States should undertake broad, sustained diplomatic engagement to advance collaboration on emerging technologies, norms, and standard setting. This will require clearer articulation of U.S. policies and standards on multiple issues."[114]

Unlike AI or cyber, biotechnologies directly implicate the human condition, carrying life-saving medical promise on the one hand, and the potential for amoral overreach and malign use on the other.[115] In 2009, Stanford political scientist Francis Fukuyama described both the fragmentary national-level approach to biotechnology regulation and the lack of consensus among nation-states about how — or even if — to create international rules or governance mechanisms around such technologies.[116]

Unlike the digital and cyber realms, the UN's current approaches to bioethics and biotechnology fall under the UNESCO umbrella, with the latter scoped primarily to the positive opportunities for achieving national development goals or fighting diseases.[117] Meanwhile, China's People's Liberation Army ("PLA") has both stated and acted on its interest in harnessing biotechnology advances to provide a potential edge in warfare — with perhaps minimal regard for the ethical implications.[118] In the absence of a Washington-led effort to start the vital conversations with other global scientific powers about the norms and appropriate boundaries for biotechnology's applications, the vacuum will pose unacceptable risks to both U.S. values and national security interests.

Lessons from the AI and cyber arenas — which themselves are still evolving and nowhere approaching enshrinement in international law by treaty or binding consensus akin to the Law of Armed Conflict or the UN Convention for the Law of the Sea[119] — may help in establishing norms for biotechnology.

Finally, the intent of rogue or other non-state actors in acquiring innovative technology unites nation-states in a quest to deny such technology to those who ignore international norms or who are not subject to deterrence. Technological innovation that requires substantial investment or specialized knowledge is not likely to be achieved by actors with limited resources. However, non-state actors will be very interested in applying the fruits of such innovation for their desired ends. Just as terrorists have explored acquiring nuclear technology, we should expect that terrorists or transnational criminals might seek to steal, or in some cases simply purchase the products of synthetic biology or AI.[120]

The United States should help develop ethical and normative frameworks for emerging dual-use technologies.

It should also engage with authoritarian adversaries such as China and Russia to find common ground and set the terms of the debate, without compromising U.S. values or principles. Doing so can increase the odds that it will have the backing of the global community to forcefully counter any unethical or amoral applications of these technologies carried out by malign actors, sovereign or otherwise.

IV. CONCLUSION

When this Subcommittee was created in the 116th Congress, we were handed a challenging responsibility: focus on, oversee, and evaluate the Intelligence Community's development and use of emerging and advanced technologies. This challenge is as important to the safety and prosperity of the United States and its allies as it is historically resonant with those who remember the triumphs and failures of the twentieth century.

The United States got it right when it mobilized the best talent in the world behind the Manhattan Project to make sure that the forces of freedom developed nuclear technology before the fascists did. The United States failed in 1957 when millions of Americans watched a Soviet satellite pass over their homes and communities. Since then, a sustained effort to maintain a technological edge has kept the United States and its allies safe and catalyzed the modern global technology economy.

Once again, the United States finds itself confronting technological innovation at a pace and scale that demands immediate attention: AI, 5G, quantum computing, and biosynthesis offer science-fiction like promise, but also previously unimaginable threats. Will the United States lead in the development of these technologies, or will it be ambushed, Sputnik-like, by a cataclysmic technological surprise? Should we work to make the present conundrum around Huawei's dominance in 5G technology a rare outlier, or are we comfortable being reactive to a menu of bad policy choices?

Legislators and other policymakers must look beyond the time-tested cure-all solution of simply spending more money. Government is far more complex and bureaucratic than it was during the Manhattan Project, and the global innovative ecosystem bears almost no similarities to that of the 1940s. The private sector is now innovating in almost every sphere and undertaking the lion's share of U.S. R&D.[121] Our global competitors and antagonists are, or soon will be, our peers in cutting edge technology. Fortunately, so are our allies and partners.

Leveraging the brainpower, ideas and products of U.S. academics and entrepreneurs is a complicated bureaucratic endeavor. In order to harness the best innovative minds distributed throughout the U.S. economy, the government must continue the sometimes-counterintuitive commitment to partnership, interaction and openness, even with other countries. Openness is a competitive advantage to democratic societies, even as it threatens authoritarian ones.

The IC, and the broader national security apparatus, must systematically reflect on the critical ingredients of American innovation, precisely because many of those ingredients, like unorthodox thinking, embrace of failure, and non-hierarchical organizations, are unusual or even anathema to government culture. Government is not naturally configured to “think different” or to “move fast and break things”.

Embracing our recommendations may involve some incremental risk. But that risk must be evaluated in the context of being a technological “also ran,” with all that that would imply for national security economic growth.

Finally, winning is important, and in some areas, critical; but it isn’t everything. The United States was fortunate to beat the fascist powers to nuclear weaponry. But the Soviets tested an atom bomb four years later. The most powerful AI, like any other software, will be easy to copy, trade, or steal.[122] The United States cannot rely on being in a position of perpetual and unilateral technological dominance. It is therefore critical that the United States double down on leading the world in the establishment of ethics and international norms that guide when, how, and why we use these incredible technologies. While we may not always be able to outspend or outman our competitors, we can – and must – do what we’ve always done: lead in the creation of a better and safer world.

APPENDIX A: SUMMARY OF RELEVANT AND SELECT REPORT RECOMMENDATIONS

National Commission for the Review of Research and Development Programs of the United States Intelligence Community	● Devote greater attention to strategic scientific and technical intelligence and use it to inform R&D plans for the IC. ● Develop a comprehensive IC R&D strategy and resource allocation process. ● Assess the long-term IC workforce needs in the context of a more competitive private sector and global marketplace and develop procedures to recruit and retain the necessary talent. ● Increase innovation and sharing with the private sector, academia, and national labs, and create research opportunities for non-U.S. citizens.[123]
Defense Innovation Board	● Reform statutes, regulations, and processes for software, enabling rapid deployment and continuous improvement of software to the field and providing increased insight to reduce the risk of slow, costly, and overgrown programs. The management and oversight of software development and acquisition must focus on different measures and adopt a quicker cadence. ● Create and maintain cross-program/cross-service digital infrastructure that enables rapid deployment, scaling, testing, and optimization of software as an enduring capability; manage them using modern development methods; and eliminate the existing hardware-centric regulations and other barriers. ● Create new paths for digital talent (especially internal talent) by establishing software development as a high-visibility, high-priority career track with specialized recruiting, education, promotion, organization, incentives, and salary. ● Change the practice of how software is procured and developed by adopting modern software development approaches, prioritizing speed as the critical metric, ensuring cyber protection is an integrated element of the entire software lifecycle, and purchasing existing commercial software whenever possible.[124]
Council on Foreign Relations	● Restore federal funding for R&D from 0.7 percent to 1.1 percent of gross domestic product, from $146 billion to $230 billion. ● Create extensive scholarships and graduate fellowships in Science, Technology, Engineering, and Math (STEM) as well as opportunities for short term service in the federal government for STEM personnel.

	● Make it easier for foreign STEM graduates of U.S. universities to remain in the United States and for immigrants to live in the United States if they start and fund new businesses. ● Improve rapid adoption of commercial and emerging technologies in the federal government through fast tracks and increased spending. ● Build a network of international science and technology partners with joint R&D efforts and shared standards.[125]
Center for Strategic and International Studies	● Identify and prioritize “must win” technologies for the United States. ● Engage with allies and partners to advance collaboration on emerging technologies, norms, and standards-setting. ● Experiment with new models for public-private partnerships and build government expertise in emerging technologies. ● Maximize the effectiveness of existing resources through data releases and funding targeted at commercial research gaps. ● Increase attention to the human dimensions of emerging technologies, including ethics, education, recruitment, and immigration.[126]
Center for a New American Security	● Foster more flexible international technology alliances that emphasize tangible economic benefits, solving specifically defined problems, and reducing preferences for spending and procuring domestically.[127] ● Increase funding for high-risk, high-reward research into areas where private industry has little incentive to invest but that hold tremendous potential for valuable new knowledge. ● Increase public and private sector STEM training and education, increase federal funding for university researchers, and create more avenues for high-skilled immigration. [128]
Center for Security and Emerging Technology	● Foster international partnerships based on R&D collaboration, counterintelligence cooperation, shared norms for emerging technology, and coordinated export controls against competitors.[129] ● Expand temporary visa and permanent residency options for skilled foreign STEM workers, and create carefully crafted immigration opportunities for entrepreneurs.[130] ● Establish direct conversations and initiatives with allies and competitors to create shared norms and deconfliction mechanisms for emerging technologies.[131]

APPENDIX B. METHODOLOGY AND LIST OF ENGAGEMENTS

Over the course of the 116th Congress, the Subcommittee convened roundtables and formal meetings in Washington, D.C., and held phone-based briefings with current and former IC and U.S. government personnel with hands-on experience. These personnel offered valuable insights into further accelerating the adoption of emerging technology to solve national security problems.

Subcommittee and Committee engagements

- February 12, 2020: Subcommittee Open Hearing, "Emerging Technologies and National Security: Posturing the U.S. Intelligence Community for Success".
- April 4, 2019: Committee roundtable with In-Q-Tel Chief Executive Officer, Chris Darby.
- June 12, 2019: Subcommittee Roundtable, Principal Deputy Director of National Intelligence Sue Gordon
- December 4, 2019: Research Directorate, National Security Agency

  December 9, 2019: Intelligence Advanced Research Projects Activity
- January 16, 2020: Defense Advanced Research Project Agency
- March 3, 2020: Directorate of Science and Technology, Central Intelligence Agency
- August 27, 2020: Kessel Run

Staff Engagements

- Jason Matheny, former Director of IARPA and founding director of Georgetown's Center for Security and Emerging Technology
- Science, Technology Assessment, and Analytics team, Governmental Accountability Office
- Massachusetts Institute of Technology
- National Institute of Standards and Technology
- Representatives from the Department of Energy's National Labs, including Sandia National Lab, Lawrence Livermore National Lab, Los Alamos National Lab, Pacific Northwest National Lab, and Idaho National Lab.
- National Security Commission on Artificial Intelligence
- CSIS Task Force
- Cyberspace Solarium Commission

Congressional Delegations and Fact-Finding Trips

To ensure that the Subcommittee solicited expert commentary from beyond Washington, it took trips to New York, Boston, and California:

- The Subcommittee met with venture capitalists in **New York** for wide-ranging conversations about geopolitical technological competition between the United States and China, the strong state of AI R&D in the U.S. private sector, and the suggestion that Washington create elite "technical teams" modeled on U.S. Special Forces, with correlating resources and rigor but whose is scoped mission of developing essential emerging technologies.

- A visit to companies and labs in **Massachusetts** including **MIT's Computer Science and Artificial Intelligence Lab, MIT Lincoln Laboratory, Forge.AI, Gingko Bioworks,** and **Forrester Research** gave the Subcommittee concrete on-the-ground examples about AI and its intersections with cybersecurity and synthetic biology with potential relevance to and applications in IC.

- A pair of trips to California offered the Subcommittee opportunities to solicit inputs from a mix of private and USG entities, including **Apple**, **Rigetti Computing, Kleiner Perkins, Lawrence Livermore National Lab,** and **NGA's Silicon Valley Outpost** on topics including quantum computing, developments in hardware, the and the vital role of venture capital in spotting and nurturing technologies – and how the U.S. government can more vigorously adopt lessons from that space.

ENDNOTES

[1] Bush, Vannevar. “Science, The Endless Frontier.” United States Government Printing Office, July 1945. https://www.nsf.gov/od/lpa/nsf50/vbush1945.htm.

[2] McRaven, William H., and James Manyika. “Innovation and National Security: Keeping Our Edge.” Council on Foreign Relations, September 2019. https://www.cfr.org/report/keeping-our-edge/.

[3] McRaven and Manyika, “Innovation and National Security: Keeping Our Edge”.

[4] “The State of U.S. Science and Engineering.” National Science Board, National Science Foundation, January 2020. https://ncses.nsf.gov/pubs/nsb20201/global-r-d.

[5] Sargent, John F. “Global Research and Development Expenditures: Fact Sheet.” Congressional Research Service, U.S. Library of Congress, April 29, 2020. https://fas.org/sgp/crs/misc/R44283.pdf.

[6] “Made in China 2025: Global Ambitions Built on Local Protections.” U.S. Chamber of Commerce, March 16, 2017. https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

[7] Raymond Perrault, Yoav Shoham, Erik Brynjolfsson, Jack Clark, John Etchemendy, Barbara Grosz, Terah Lyons, James Manyika, Saurabh Mishra, and Juan Carlos Niebles, “The AI Index 2019 Annual Report”, AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, December 2019; Yui, Yuen. “Is China the Leader in Quantum Communications?” May 15, 2020. https://www.insidescience.org/news/china-leader-quantum-communications.

[8] “Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community” (2016). https://www.intelligence.senate.gov/sites/default/files/commission_report.pdf.

[9] Simonite, Tom. “The WIRED Guide to Quantum Computing.” Wired, August 24, 2018. https://www.wired.com/story/wired-guide-to-quantum-computing/.

[10] Kolodny, Lora. “These Robots Handle Dull and Dangerous Work Humans Do Today — and Can Create New Jobs.” CNBC Upstart 100. CNBC, October 10, 2018. https://www.cnbc.com/2018/10/09/robots-handle-dull-dangerous-work-creating-new-jobs-for-humans.html; Liu, Nan, Zhongheng Zhang, Andrew Fu Wah Ho, and Marcus Eng Hock Ong. “Artificial Intelligence in Emergency Medicine.” Journal of Emergency and Critical Care Medicine 2 (October 2018). http://jeccm.amegroups.com/article/view/4700/5245; Swayne, Matt. “Artificial Intelligence That Pinpoints Swift-Changing Weather Areas Could Result in More Accurate Weather Forecasts.” Futurity, August 23, 2019. https://www.futurity.org/weather-forecasts-artificial-intelligence-2141972/.

[11] Work, Robert O., and Shawn Brimley. “20YY: Preparing for War in a Robotic Age.” Center for a New American Security, January 2014. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_20YY_WorkBrimley.pdf.

[12] Begley, Sharon. “Synthetic Biologists Think They Can Develop a Better Coronavirus Vaccine Than Nature Could.” Scientific American, March 9, 2020. https://www.scientificamerican.com/article/synthetic-biologists-think-they-can-develop-a-better-coronavirus-vaccine-than-nature-could/; Paul, Eve Turow. “You Need to Know: All About Synthetic Biology Foods.” HuffPost, February 16, 2016. https://www.huffpost.com/entry/you-need-to-know-all-abou_b_9237578.

[13] Hessel, Andrew, Marc Goodman, and Steven Kotler. “Hacking the President’s DNA.” The Atlantic, November 2012. https://www.theatlantic.com/magazine/archive/2012/11/hacking-the-presidents-dna/309147/.

[14] Kania, Elsa B. “Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy.” Center for a New American Security, November 7, 2019. https://www.cnas.org/publications/reports/securing-our-5g-future.

[15] Pongratz, Stefan. “Key Takeaways – Worldwide Telecom Equipment Market 2018.” Dell'Oro Group, March 4, 2019. https://www.delloro.com/telecom-equipment-market-2018-2/.

[16] Fung, Brian. “How China’s Huawei Took the Lead over U.S. Companies in 5G Technology.” The Washington Post, April 10, 2019. https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/; Marek, Sue. “Huawei’s 5G RAN Portfolio Beats Ericsson, Nokia and Others, Report Says.” FierceWireless, June 25, 2019. https://www.fiercewireless.com/wireless/huawei-s-5g-ran-portfolio-beats-ericsson-nokia-and-others-report-says.

[17] Halpern, Sue. “The Terrifying Potential of the 5G Network.” The New Yorker, April 26, 2019. https://www.newyorker.com/news/annals-of-communications/the-terrifying-potential-of-the-5g-network.

[18] United States House of Representatives Permanent Select Committee on Intelligence, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (2012).

[19] Brose, Christian. The Kill Chain: Defending America in the Future of High-Tech Warfare. New York, NY: Hachette Books, 2020.

[20] Andreessen, Marc. "Why Software Is Eating the World." The Wall Street Journal, August 20, 2011. https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.

[21] "Historical Trends in Federal R&D." American Association for the Advancement of Science, 2020. https://www.aaas.org/programs/r-d-budget-and-policy/historical-trends-federal-rd.

[22] McRaven and Manyika,"Innovation and National Security: Keeping Our Edge."

[23] Sargent.

[24] "Historical Trends in Federal R&D."

[25] Thilo Hanemann, Daniel H. Rosen, Cassie Gao, and Adam Lysenko. "Two-Way Street: 2020 Update US-China Investment Trends." Rhodium Group, May 11, 2020. https://arraysproduction-0dot22.s3.amazonaws.com/rhodiumgroup/assets/icon/TWS-2020_Report_8May2020_Final.pdf

[26] Moore, Jack. "In Fierce Battle for Cyber Talent, Even NSA Struggles to Keep Elites on Staff." Nextgov, April 14, 2015. https://www.nextgov.com/cybersecurity/2015/04/fierce-battle-cyber-talent-even-nsa-struggles-keep-elites-staff/110158/.; Metz, Cade. "Tech Giants Are Paying Huge Salaries for Scarce A.I. Talent." The New York Times, October 22, 2017. https://www.nytimes.com/2017/10/22/technology/artificial-intelligence-experts-salaries.html.

[27] 50 U.S.C. § 3049a (2017).

[28] 10 U.S.C. § 1599h (2019).

[29] 18 U.S.C. § 202. U.S. Office of Government Ethics. *Special Government Employees.* Accessed September 1, 2020. https://www.oge.gov/Web/OGE.nsf/Resources/Special+Government+Employees.

[30] Office of the Director of National Intelligence. "Intelligence Community Directive Number 623." October 16, 2008. https://www.dni.gov/files/documents/ICD/ICD_623.pdf.

[31] Wagner, Erich. "OPM Issues Regulations for Feds' Paid Parental Leave," August 7, 2020. https://www.govexec.com/pay-benefits/2020/08/opm-issues-regulations-feds-paid-parental-leave/167555/.

[32] 10 U.S.C § 1599h (2019).

[33] "Pay & Leave: Student Loan Repayment." U.S. Office of Personnel Management, 2020. https://www.opm.gov/policy-data-oversight/pay-leave/student-loan-repayment/.

[34] "Tour of Duty Hiring in the Federal Government." Institute for Defense Analyses, June 2019. https://www.ida.org/-/media/feature/publications/t/to/tour-of-duty-hiring-in-the-federal-government/d10700final.ashx.

[35] Booz, Michael. "These 3 Industries Have the Highest Talent Turnover Rates." LinkedIn Talent Blog, March 15, 2018. https://business.linkedin.com/talent-solutions/blog/trends-and-research/2018/the-3-industries-with-the-highest-turnover-rates.

[36] Kyzer, Lindy. "It's Time to Reform Intelligence Community Hiring Practices." Government Executive, December 12, 2019. https://www.govexec.com/management/2019/12/its-time-reform-intelligence-community-hiring-practices/161844/.; Lopez, C. Todd. "Defense Digital Service Delivers Mission-Aligned Tech for DOD." U.S. Department of Defense, May 29, 2019. https://www.defense.gov/Explore/News/Article/Article/1858615/defense-digital-service-delivers-mission-aligned-tech-for-dod/.

[37] 10 U.S.C. § 2192b (2020); 10 U.S.C. § 2194 (2020).

[38] U.S. Congress, House, *Intelligence Authorization Act for Fiscal Year 2021 § 603*, HR 7856, 116th Cong., 2nd sess., introduced in House July 30, 2020, https://www.congress.gov/bill/116th-congress/house-bill/7856.

[39] Government Accountability Office, "Personnel Security Clearances: Additional Actions Needed to Ensure Quality, Address Timeliness, and Reduce Investigation Backlog." December 2017. GAO-18-29. https://www.gao.gov/assets/690/689278.pdf.; Government Accountability Office, "High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress in High-Risk Areas." March 2019. GAO-19-1575P. https://www.gao.gov/assets/700/697245.pdf.

[40] President's Management Agenda, "Security Clearance, Suitability/Fitness, and Credentialing Reform." July 2020. https://www.performance.gov/CAP/action_plans/july_2020_Security_Suitability.pdf.

[41] Barton, Michael James. “Government Clearance Backlog Threatens Our National Security.” The Hill, September 13, 2017. https://thehill.com/opinion/national-security/350424-government-clearance-backlog-threatens-our-national-security.

[42] Weinbaum, Courtney, Arthur Chan, Karlyn D. Stanley, and Abby Schendt. ” Moving to the Unclassified: How the Intelligence Community Can Work from Unclassified Facilities.” RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2024.html.; Hitchens, Theresa. “COVID-19: NGA Pumps Unclassified Data Use, Says Vice Adm. Sharp.” Breaking Defense, April 22, 2020. https://breakingdefense.com/2020/04/covid-19-nga-pumps-unclassified-data-use-says-vice-adm-sharp/.

[43] “Learn about NSA's University-Level Research Partnerships.” National Security Agency | Central Security Service, 2020. https://www.nsa.gov/resources/students-educators/research-partnership/.

[44] Kerr, William. “High-Skilled Immigration and the Growing Concentration of US Innovation.” Centre for Economic Policy Research, October 26, 2018. https://voxeu.org/article/high-skilled-immigration-and-growing-concentration-us-innovation.; Ozden, Caglar. “Global Talent Flows: Causes and Consequences of High-Skilled Migration.” World Bank Blogs, May 31, 2017. https://blogs.worldbank.org/developmenttalk/global-talent-flows-causes-and-consequences-high-skilled-migration.

[45] Tabansky, Lior. Essay. In Cybersecurity in Israel, edited by Isaac Ben Israel, 15–30. New York, NY: Springer International Publishing, 2015.

[46]Huang, Tina, and Zachary Arnold, “Immigration Policy and the Global Competition for AI Talent.” Center for Security and Emerging Technology, June 2020, https://cset.georgetown.edu/research/immigration-policy-and-the-global-competition-for-ai-talent/.

[47] “The State of U.S. Science and Engineering: U.S. S&E Workforce.” National Science Board, National Science Foundation, January 2020. https://ncses.nsf.gov/pubs/nsb20201/u-s-s-e-workforce#foreign-born-scientists-and-engineers.

[48] Ledford, Ed. “Two Big Takeaways from the CIA Hiring Processes.” ClearanceJobs, February 6, 2017. https://news.clearancejobs.com/2017/02/06/two-big-takeaways-cia-hiring-processes/.

[49] United States Intelligence Community, “Intelligence Community Tips for the Hiring & Security Clearance” Process . https://iccae.ku.edu/sites/iccae.ku.edu/files/docs/Security-Takeaways-Handout.pdf.

[50] Jordan, Miriam. “Wait Times for Citizenship Have Doubled in the Last Two Years.” The New York Times, February 21, 2019. https://www.nytimes.com/2019/02/21/us/immigrant-citizenship-naturalization.html.

[51] Huang and Arnold, “Immigration Policy and the Global Competition for AI Talent.”

[52] Office of the Director of National Intelligence, The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines § (2019). https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf; Gordon, Susan, “Roundtable with Principal Deputy Director of National Intelligence Susan Gordon” (roundtable discussion, House Permanent Select Committee on Intelligence Subcommittee on Strategic Technology and Advanced Research, Washington, DC, June 12, 2019); Darby, Chris, “Roundtable with In-Q-Tel CEO Chris Darby” (roundtable discussion, House Permanent Select Committee on Intelligence, Washington, DC, April 4, 2019.

[53] Strout, Nathan. “3 Challenges Facing the National Security Community in the Information Age.” C4ISRNET, June 28, 2019. https://www.c4isrnet.com/information-warfare/2019/06/28/3-challenges-facing-the-national-security-community-in-the-information-age/.

[54] Whittaker, Zack. “Five Years On, Snowden Inspired Tech Giants to Change, Even If Governments Wouldn't.” ZDNet, June 6, 2018. https://www.zdnet.com/article/edward-snowden-five-years-on-tech-giants-change/; Kang, Cecilia, Nicholas Fandos and Mike Isaac. “Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill.” *The New York Times*, October 31, 2017. https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html; Zegart, Amy, and Kevin Childs. “The Divide Between Silicon Valley and Washington Is a National-Security Threat.” *The Atlantic*, December 13, 2018. https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.

[55] Stewart, Christopher S., and Mark Maremont. "Twitter Bars Intelligence Agencies From Using Analytics Service." *The Wall Street Journal*, May 8, 2016. https://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682.

[56] Valinsky, Jordan. "Google Drops $10 Billion Bid for Pentagon Contract." *CNN Business*, October 9, 2018. https://www.cnn.com/2018/10/09/tech/google-defense-contract/index.html.

[57] NDSS Symposium. "NDSS 2019 - Keynote: Modern Challenges for Cyber Defense - Dr. Deborah Frincke," YouTube video, 55:09, April 2, 2019, https://www.youtube.com/watch?v=5a2w6m6OP50; ICME Studio. "Data Science Supporting National Security | Dr. Deborah Frincke | WiDS 2017," YouTube video, 40:15, March 20, 2017, https://www.youtube.com/watch?v=Au8THpZyzAo.

[58] Joyce, Rob. "Improving and Making the Vulnerabilities Equities Process Transparent is the Right Thing to Do." The White House, November 15, 2017. https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/; Vulnerabilities Equities Process Highlights" Electronic Frontier Foundation, July 8, 2010. https://www.eff.org/document/vulnerabilities-equities-process-highlights-782010; "Vulnerabilities Equities Policy and Process for the United States Government." The White House, November 17, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[59] "CVE-2020-0601 | Windows CryptoAPI Spoofing Vulnerability." Security Update Guide, Microsoft Security Response Center, January 14, 2020. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-0601.

[60] Dreyfuss, Emily. "Top US Intelligence Official Sue Gordon Wants Silicon Valley on Her Side." Wired, November 9, 2018. https://www.wired.com/story/sue-gordon-us-intelligence-public-private-google-amazon/.

[61] RSA Conference. "Strategic Competition: The Rise of Persistent Presence and Innovation." YouTube video, 46:02, March 6, 2019, https://www.youtube.com/watch?v=Apd2ReXB6vk;
Black Hat. "Black Hat USA 2013 Keynote – Gen. Alexander," YouTube video, 53:38, July 31, 2013, https://youtu.be/xvVIZ4OyGnQ; Madrigal, Alexis, Jason Matheny, and Dario Gil. "Myths and Realities of the Next Computing Revolution." Discussion Event, Aspen Ideas Festival 2018, Aspen, CO, June 30, 2018.

[62] See, for example, "General Paul M. Nakasone." U.S. Department of Defense. Accessed August 4, 2020. https://www.defense.gov/Our-Story/Biographies/Biography/Article/1531067/general-paul-m-nakasone/; see also "Gina Haspel." White House. Accessed August 4, 2020. https://www.whitehouse.gov/people/gina-haspel/; see also "Lieutenant General Scott D. Berrier," AFCEA, accessed August 4, 2020, https://www.afcea.org/event/sites/default/files/files/Berrier%2C%20LTG%20Scott%20D_%20Bio.pdf; see also "Vice Admiral Robert D. Sharp, Director." National Geospatial-Intelligence Agency. Accessed August 4, 2020. https://www.nga.mil/About/Leadership/Pages/VADMSharp.aspx.

[63] "Our History." In-Q-Tel, n.d. https://www.iqt.org/our-history/.

[64] Gazis, Olivia. "In-Q-Tel President Chris Darby on the Intelligence Community's Innovation Challenges." CBS News, April 24, 2019. https://www.cbsnews.com/news/intelligence-matters-in-q-tel-president-chris-darby-on-the-intelligence-communitys-innovation-challenges/; Szoldra, Paul. "14 Cutting Edge Firms Funded by the CIA." Business Insider, September 21, 2016. https://www.businessinsider.com/companies-funded-by-cia-2016-9.

[65] Farr, Christina. "Why In-Q-Tel Investment Is a 'Stamp of Approval' for Enterprise Startups." VentureBeat, April 25, 2013. https://venturebeat.com/2013/04/25/why-in-q-tel-investment-is-a-stamp-of-approval-for-enterprise-startups/.

[66] "How We Work." In-Q-Tel, n.d. https://www.iqt.org/how-we-work/venture-capital/

[67] Yaraghi, Niam. "Doomed: Challenges and Solutions to Government IT Projects," July 29, 2016. https://www.brookings.edu/blog/techtank/2015/08/25/doomed-challenges-and-solutions-to-government-it-projects/.

[68] Nyce, Caroline Mimbs. "The Winter Getaway That Turned the Software World Upside Down." The Atlantic. Atlantic Media Company, December 8, 2017. https://www.theatlantic.com/technology/archive/2017/12/agile-manifesto-a-history/547715/.

[69] McQuade, Murray, Louie, Medin, et al. "Software Is Never Done."

[70] "Report of the Defense Science Board Task Force on Military Software." Defense Science Board, U.S. Department of Defense, September 1987. https://apps.dtic.mil/dtic/tr/fulltext/u2/a188561.pdf.

[71] McQuade, Murray, Louie, Medin, et al. "Software Is Never Done."

[72] Serbu, Jared. "Pentagon's Number-Two Officer Vows to Fix Software Acquisition 'Nightmare'." Federal News Network, January 21, 2020. https://federalnewsnetwork.com/defense-main/2020/01/pentagons-number-two-officer-vows-to-fix-software-acquisition-nightmare/; Charette, Robert N. "U.S. Air Force Blows $1 Billion on Failed ERP Project." IEEE Spectrum: Technology, Engineering, and Science News, November 15, 2012. https://spectrum.ieee.org/riskfactor/aerospace/military/us-air-force-blows-1-billion-on-failed-erp-project.

[73] "The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines." Office of the Director of National Intelligence, January 16, 2019. https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf.

[74] Mitchell, Billy. "Air Force's Kessel Run Has Admirers Elsewhere in the Military." *FedScoop*, November 16, 2018. https://www.fedscoop.com/kessel-run-pentagon-military/.

[75] Newell, Benjamin. "Kessel Run Announces Hiring Event," January 7, 2019. https://www.af.mil/News/Article-Display/Article/1725094/kessel-run-announces-hiring-event/; "Direct Hire Authority." U.S. Office of Personnel Management. Accessed September 1, 2020. https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/.

[76] U.S. Merit Systems Protection Board, "Direct Hiring Authority: A Look at the Numbers." *Issues of Merit*, February 2019. 2. Accessed September 1, 2020. https://www.mspb.gov/MSPBSEARCH/viewdocs.aspx?docnumber=1585933&version=1591693&application=ACROBAT.

[77] Pomerleau, Mark. "How the Air Force's New Software Team Is Proving Its Worth." C4ISRNET, January 14, 2019. https://www.c4isrnet.com/it-networks/2019/01/14/how-the-air-forces-new-software-team-is-proving-its-worth/.

[78] Wallace, Mark. "The U.S. Air Force Learned to Code—and Saved the Pentagon Millions." *Fast Company*, July 5, 2018. https://www.fastcompany.com/40588729/the-air-force-learned-to-code-and-saved-the-pentagon-millions.

[79] Cohen, Rachel S. "The Air Force Software Revolution." Air Force Magazine, September 1, 2019. https://www.airforcemag.com/article/the-air-force-software-revolution/.

[80] Mitchell, Billy. "Intelligence CIOs Still Figuring out How to Be Cost-Effective in the Cloud." FedScoop. August 20, 2019. https://www.fedscoop.com/intelligence-community-cloud-computing-dynamic-costs/.

[81] "Promoting DoD's Culture of Innovation," 115th Congress (April 17, 2018) (Dr. Eric Schmidt).

[82] National Defense Authorization Act for Fiscal Year 2020, P.L. 116-92 § 5306 (2019).

[83] Cox, Amy G., Nancy Y. Moore, and Clifford A. Grammich. " Identifying and Eliminating Barriers Faced by Nontraditional Department of Defense Suppliers." RAND Corporation, 2014. https://apps.dtic.mil/dtic/tr/fulltext/u2/a609831.pdf.

[84] Lawlor, Maryann. "Capturing Intelligence Contracts Poses Challenges To Small Businesses." SIGNAL Magazine. Armed Forces Communications and Electronics Association, June 2009. https://www.afcea.org/content/capturing-intelligence-contracts-poses-challenges-small-businesses-0.

[85] Boyd, Aaron. "The Scary New Contracting Model That Isn't Scary or New." Nextgov.com. Nextgov, July 19, 2018. https://www.nextgov.com/it-modernization/2018/03/otas-scary-new-contracting-model-isnt-scary-or-new/146964/.

[86] Gallo, Marcy E. "Federally Funded Research and Development Centers (FFRDCs): Background and Issues for Congress." Congressional Research Service, U.S. Library of Congress, April 3, 2020. https://crsreports.congress.gov/product/pdf/R/R44629.

[87] U.S. Department of Energy, "Transition: 2016," Book 1, "Corporate Overview." June 2019. https://www.energy.gov/sites/prod/files/2017/04/f34/MAAdm_TransitionBook1-CorporateOverview2016.pdf.

[88] Ibid.

[89] DeVine, Michael E. "United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits." Congressional Research Service, U.S. Library of Congress, May 15, 2019. https://fas.org/sgp/crs/intel/R45720.pdf.

[90] Du Cluzel, Francois. "How NATO is Innovating Toward the Future." The Cipher Brief, May 14, 2020. https://www.thecipherbrief.com/column_article/how-nato-is-innovating-toward-the-future.

[91] U.S. Mission to NATO. “The Maritime Unmanned Systems Innovation and Coordination Cell Announces the Formation of the MUS Innovation Advisory Board”, May 11, 2020. https://nato.usmission.gov/press-release-the-maritime-unmanned-systems-innovation-and-coordination-cell-music2-announces-the-formation-of-the-mus-innovation-advisory-board/.

[92] Roberson, T. M., and A. G. White. "Charting the Australian quantum landscape." Quantum Science and Technology 4, no. 2 (2019): 020505., https://iopscience.iop.org/article/10.1088/2058-9565/ab02b4/pdf.

[93] Melissa Flagg, "Global R&D and a New Era of Alliances." Center for Security and Emerging Technology, June 2020, cset.georgetown.edu/research/global-rd-and-a-new-era-of-alliances/.

[94] Katz, Brian. “The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for U.S. Intelligence.” Center for Strategic and International Studies, April 2020. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200417_Katz_IntelligenceEdge_WEB%20FINAL.pdf?dWNvglzd.By4.c6nic7X5xkNmOf4t1I4.

[95] Office of the Director of National Intelligence, Policy Memorandum Number 2005-800-1 § (2006). https://www.dni.gov/files/documents/IC%20Policy%20Memos/2006-01-06IntelCommunityPolicyMemorandum2005-800-1.pdf.

[96] Office of the Director of National Intelligence, Information Management Office, ODNI Congressional Budget Justification Book (CBJB) for Fiscal Year 2009 (Washington, 2018), 162, https://fas.org/irp/dni/cbjb-2009.pdf.

[97] “Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community.”

[98] Zoeller, Jack, Barbara Barrett, Mel Immergut, Philip Odeen, and Atul Vashishta. “Public-Private Collaboration in the Department of Defense.” Defense Business Board, January 19, 2012. https://dbb.defense.gov/Portals/35/Documents/Reports/2012/FY12-4_Public_Private_Collaboration_in_the_Department_of_Defense_2012-7.pdf.

[99] “Defense Innovation Board: About.” U.S. Department of Defense, 2016. https://innovation.defense.gov/About1/.

[100] McQuade, Murray, Louie, Medin, et al. “Software Is Never Done.”
; Chappellet-Lanier, Tajha. “Pentagon’s Joint AI Center Is ‘Established,’ but There’s Much More to Figure Out.” FedScoop, July 20, 2018. https://www.fedscoop.com/dod-joint-ai-center-established/.

[101] “DOD Adopts Ethical Principles for Artificial Intelligence.” U.S. Department of Defense - Newsroom, February 24, 2020. U.S. Department of Defense. https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

[102] Fung, Brian. “How China’s Huawei Took the Lead over U.S. Companies in 5G Technology.” The Washington Post, April 10, 2019. https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/; Raposo, Vera Lucia. “The First Chinese Edited Babies: A Leap of Faith in Science.” JBRA Assisted Reproduction 23, no. 3 (September 2019): 197–99. https://doi.org/10.5935/1518-0557.20190042.

[103] Fruhlinger, Josh. “The OPM Hack Explained: Bad Security Practices Meet China's Captain America.” CSO Online, February 12, 2020. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html; Korte, Gregory. “Putin Ordered Hacking to Help Trump, Intelligence Report Says.” USA Today, January 7, 2017. https://www.usatoday.com/story/news/politics/2017/01/06/putin-ordered-hacking-help-trump-intelligence-report-says/96260102/.

[104] Uberti, David. “Marriott Reveals Breach That Exposed Data of Up to 5.2 Million Customers.” Wall Street Journal, March 31, 2020. https://www.wsj.com/articles/marriott-reveals-breach-that-exposed-data-of-up-to-5-2-million-customers-11585686590; McCoy, Kevin. “Target to Pay $18.5m for 2013 Data Breach That Affected 41 Million Consumers.” USA Today, May 23, 2017. https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/; “Information on the Capital One Cyber Incident.” Capital One Financial Corporation, September 23, 2019. https://www.capitalone.com/facts2019/; Davis, Jessica. “11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach.” Health IT Security, June 3, 2019. https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach; Federal Bureau of Investigation, 2019 Internet Crime Report. (Washington, 2020) https://pdf.ic3.gov/2019_IC3Report.pdf.

[105] "U.S. Cyberspace Solarium Commission Final Report." March 2020; "Tallinn Manual 2.0." Research. NATO Cooperative Cyber Defence Centre of Excellence, 2017. https://ccdcoe.org/research/tallinn-manual/. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

[106] United Nations, General Assembly, *Advancing responsible State behaviour in cyberspace in the context of international security,* A/RES/73/266 (22 December 2018), available from https://undocs.org/A/RES/73/266

[107] Sukumar, Arun M. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" Lawfare, July 4, 2017. https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

[108] Lauber, Jürg. "Letter from Open-Ended Working Group Chair to United Nations." UNARM. United Nations Office for Disarmament Affairs, July 16, 2020. https://front.un-arm.org/wp-content/uploads/2020/07/200716-oewg-chair-letter-on-new-roadmap.pdf.

[109] United Nations, General Assembly, *Advancing responsible State behaviour in cyberspace in the context of international security,* A/C.1/73/L.37 (18 Oct 2018), available from https://undocs.org/A/C.1/73/L.37.

[110] Office of the Director of National Intelligence, *The IC Principles of Artificial Intelligence Ethics* (Washington, 2020), https://www.dni.gov/files/ODNI/documents/Principles_of_AI_Ethics_for_the_Intelligence_Community.pdf.; Office of the Director of National Intelligence, *Artificial Intelligence Ethics Framework for the Intelligence Community* (Washington, 2020), https://www.dni.gov/files/ODNI/documents/AI_Ethics_Framework_for_the_Intelligence_Community_10.pdf.

[111] "DOD Adopts Ethical Principles for Artificial Intelligence." U.S. Department of Defense - Newsroom, February 24, 2020. U.S. Department of Defense. https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

[112] National Security Commission on Artificial Intelligence, "Interim Report" (November 2019). https://www.nscai.gov/reports.

[113] Ibid.

[114] Brannen, Haig, Schmidt, and Hicks. "Twin Pillars: Upholding National Security and National Innovation in Emerging Technologies Governance."

[115] Chakraborty, Sweta. "Promise and Peril: The Biotech Security Dilemma," August 21, 2017. https://warroom.armywarcollege.edu/articles/promise-peril-security-dilemma-biotechnology/.

[116]Fukuyama, Francis. "Gene Regime." Foreign Policy, November 13, 2009. https://foreignpolicy.com/2009/11/13/gene-regime/.

[117] United Nations Educational, Scientific, and Cultural Organization. "Biotechnology." http://www.unesco.org/new/en/natural-sciences/science-technology/basic-sciences/life-sciences/biotechnology/.

[118] Kania, Elsa B., and Wilson VornDick. "Weaponizing Biotech: How China's Military Is Preparing for a 'New Domain of Warfare'." Defense One. Defense One, April 14, 2020. https://www.defenseone.com/ideas/2019/08/chinas-military-pursuing-biotech/159167/.

[119] "Law of Armed Conflict (LOAC)." Peterson Air Force Base. U.S. Air Force Peterson Air Force Base Legal Office, 2016. https://www.peterson.af.mil/Portals/15/documents/Units/JudgeAdvocate/AFD-160210-019.pdf; United Nations, *Convention on the Law of the Sea,* 16 November 1982, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

[120] Bunn, Matthew, Yuri Morozov, Rolf Mowatt-Larsen, Simon Saradzhyan, William Tobey, Viktor I. Yesin, and Pavel S. Zolotarev. "The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism." Belfer Center for Science & International Affairs, May 2011. https://www.belfercenter.org/sites/default/files/files/publication/Joint-Threat-Assessment%20ENG%2027%20May%202011.pdf; Flynn, Carrick. " Recommendations on Export Controls for Artificial Intelligence." Center for Security and Emerging Technologies, February 2020. https://cset.georgetown.edu/wp-content/uploads/Recommendations-on-Export-Controls-for-Artificial-Intelligence.pdf.

[121] "Historical Trends in Federal R&D."

[122] Flynn,. "Recommendations on Export Controls for Artificial Intelligence.".

[123] Ibid.

[124] McQuade, J. Michael, Richard M. Murray, Gilman Louie, Milo Medin, Jennifer Pahlka, and Trae Stephens. "Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage." Defense Innovation Board, U.S. Department of Defense, May 3, 2019. https://media.defense.gov/2019/May/01/2002126689/-1/-1/0/SWAP%20COMPLETE%20REPORT.PDF

[125] McRaven and Manyika.

[126] Brannen, Samuel J., Christian S. Haig, Katherine Schmidt, and Kathleen H. Hicks. "Twin Pillars: Upholding National Security and National Innovation in Emerging Technologies Governance." Center for Strategic and International Studies, January 23, 2020. https://www.csis.org/analysis/twin-pillars-upholding-national-security-and-national- innovation-emerging-technologies.

[127] Kliman, Daniel, Ben FitzGerald, Kristine Lee, and Joshua Fitt. "Forging an Alliance Innovation Base." Center for a New American Security, March 2020. https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Alliance-Innovation-Base-Final.pdf?mtime=20200329174909.

[128] Rasser, Martjin, Megan Lamberth, Ainikki Riikonen, Chelsea Guo, Michael Horowitz, and Paul Scharre. "The American AI Century: A Blueprint for Action." Center for a New American Security, December 17, 2019. https://www.cnas.org/publications/reports/the- american-ai-century-a-blueprint-for-action.

[129] Imbrie, Andrew, Ryan Fedasiuk, Catherine Aiken, Tarun Chhabra, and Husanjot Chahal. "Agile Alliances: How the United States and Its Allies Can Deliver a Democratic Way of AI." Center for Security and Emerging Technology. Georgetown University, February 2020. https://cset.georgetown.edu/wp-content/uploads/CSET-Agile-Alliances.pdf.

[130] Huang and Arnold, "Immigration Policy and the Global Competition for AI Talent."

[131] Andrew Imbrie and Elsa B. Kania, "AI Safety, Security, and Stability Among Great Powers: Options, Challenges, and Lessons Learned for Pragmatic Engagement" (Center for Security and Emerging Technology, December 2019), cset.georgetown.edu/research/ai-safety-security-and-stability-among-great-powers-options-challenges-and-lessons-learned-for-pragmatic-engagement/.

MINORITY VIEWS

Report on Rightly Scaled, Carefully Open, Infinitely Agile: Reconfiguring to Win the Innovation Race in the Intelligence Community

The Majority-led Subcommittee STAR "Report" on *Rightly Scaled, Carefully Open, Infinitely Agile: Reconfiguring to Win the Innovation Race in the Intelligence Community* leverages the findings and recommendations of many existing research papers, commissions and HPSCI engagements over the past 18 months.

While the report effectively collates areas of improvement for Intelligence Community innovation, the Minority believes it would have benefited from a discussion on intellectual theft conducted by China, and other adversary nations and how the IC could address these threats. This represents a major obstacle to IC efforts to maintain US technological and innovative advantage.

The Minority's ability to address issues like China's intellectual theft in the report were constrained by the Majority's partisan practices. Minority members and staff were not included in the creation of the reports' scoping document, or in planning the oversight activities to collect the information that would eventually be included in the report. While the Minority members and staff were invited to events; the events were not "tied" to a report. Notification of events such as interviews, and travel, were often short notice precluding their involvement due to scheduling conflicts. In fact, the Minority Ranking member of the STAR Sub-Committee was not aware of the report itself, until it was handed to him at the conclusion of a committee business meeting

We hope that in the future, Committee reports are worked in a cooperative fashion with full involvement of the Minority members and staff to ensure a bi-partisan report that achieves its full potential.