National Security and the Innovation Ecosystem
By James Andrew Lewis

Executive Summary
Technological leadership has been a key part of U.S. power for decades. However, the requirements for leadership have changed. Emerging technologies are reshaping economies, societies, and warfare, but this technology will be designed by the private sector for commercial markets. The United States may not be the leader in all, and it faces intense competition.

This change in how the United States creates new technology has also changed the relationship between national security and innovation. Previous reports in this series showed that innovation in the United States is strong but has shifted to the private sector. The national security community needs new approaches to acquire innovative commercial technologies.

This is not a report on acquisitions reform—a complex issue where there has been progress but much still needs to be done. This report examines how to better connect the national security community to the dynamic U.S. innovation system, a goal first set in 2015 by Secretary of Defense Ash Carter, and lays out recommendations on the changes in funding, processes, and culture to strengthen that connection.

FUNDING
Funding provides an indicator of seriousness and intent. Nontraditional innovation programs for national security receive less than 1 percent of acquisitions funding. Companies in healthcare and information technology spend the most—on average a little more than 20 percent of their total revenue goes to research and development (R&D). Defense and aerospace companies spend on average only about 2.9 percent. It is safe to say that every major sector except telecommunications outspends the Department of Defense (DOD) when it comes to innovation. Looking at DOD spending in aggregate, there has not been a shift from large defense primes to nontraditional vendors.

The return on investment and the likelihood of success in national security missions could be increased if the United States improves its connection to the nontraditional innovators and significantly increases funding to nontraditional organizations.
CULTURE
Innovation requires more than R&D. The other half of the story is entrepreneurship—the willingness of individuals to take risks. It is the combination of innovation and entrepreneurship that explains the United States’ success in innovation. Many analysts have noted that the national security community is risk averse. The current system excels at doing what it was designed for: building major weapons systems using a steady, risk-minimizing approach. But this is not the way to acquire commercial innovation.

Creating an increased tolerance for risk is a broadly accepted goal for strengthening the national security community’s ability to acquire new technologies. The problem is that after more than a decade of trying to change culture, progress has been slow. A quicker solution is to expand or create new organizations. The United States can build on existing innovation organizations like AFWERX, the Defense Innovation Unit (DIU), NavalX, SOFWerx, and others. While all differ in varying degrees in their missions and authorities, they offer a better way to acquire innovation. But they are small, underfunded, and understaffed. The best way to change culture is to expand these groups and make sure they have sufficient funding and the right authorities.

PROCESS AND AUTHORITIES
A new approach to acquiring innovation will require modifying some processes and authorities, expanding others, and, in some instances, creating new ones. There are fears that simplifying processes for acquiring innovation could weaken oversight. A better case could be made that current oversight requirements can be reduced without harm.

The national security community has been reluctant to use existing authorities to acquire new technologies. This reflects problems of funding and culture. A first step is for Congress and the Biden administration to mandate greater use of existing authorities for acquiring innovative technology. The two most important of these existing authorities are found in Federal Acquisition Regulations (FAR) System Part 12 (the acquisition of commercial items and commercial “off-the-shelf” items) and expanded use of the Other Transaction Authority (OTA). These offer faster, more flexible ways to invest in and acquire innovative technologies.

The template for progress is to copy the private sector. This means faster timelines and greater flexibility. There is no real way to sync innovation and a multi-year Program Objective Memorandum (POM) process. Innovation organizations should have discretionary funding to invest and be able to own equity in start-ups to better partner with private sector investors and entrepreneurs. In-Q-Tel, the CIA-funded venture capital (VC) fund, may not be a perfect model, but it provides useful lessons. Rather than reworking the FAR system, Congress should provide new acquisition authorities (and funding) to acquire innovation.

OPEN QUESTIONS
The central recommendations in this report are to increase funding, create alternative organizations, mandate use of existing authorities, and provide new authorities that enable new approaches modeled on business. Doing all this would accelerate the acquisition of new technology by the national security community and improve the United States’ ability to compete with China.

However, this would still leave a number of open questions. These include the extent to which funding for nontraditional innovation should be made mandatory, perhaps by having Congress set a fixed allocation. A second issue is whether the United States should seek to consolidate the many nontraditional organizations. Finally, a nontraditional approach to innovation would benefit if the United States brought in trusted partners and close allies. There are many proposals for this, and the easiest place to start might be with the Five Eyes—an intelligence alliance between Australia, Canada, New Zealand, the United Kingdom, and the United States—but all are in early states of discussion.
CONGRESS IS KEY TO CHANGE
The imperative for change is clear. The United States is competing with powerful authoritarian states who intend to reorder the world to suit their interests and values. While the United States is well placed in the innovation race, maintaining U.S. technological advantage in national security requires new ways to acquire commercial innovation.

The need to change funding, culture, processes, and authorities all leads back to Congress. Making the national security community more “innovation friendly” requires congressional action and oversight. New funding priorities, mandates to buy commercial technology, and new authorities for nontraditional organizations can move the United States along the path identified years ago of harnessing the powerful private sector engine of U.S. innovation to strengthen national security.

A New Model of Innovation and National Security
Technological leadership has been a key component of U.S. power for decades. However, the requirements for maintaining that leadership have changed. The United States faces intense competition from China, which has emphasized expanding its own innovation capabilities and using them for national security purposes in accordance with its military-civil fusion strategy. More importantly, how the United States obtains innovative new technologies has changed. Such technologies will be created in the private sector for commercial markets, in what this report calls the national innovation ecosystem.¹

This transforms how the United States innovates for national security. It alters the relationship between national security and innovation and changes the requirements for maintaining the U.S. technological lead. The traditional methods of acquiring technology for national security are less effective in a decentralized, market-oriented system. Previous reports in this series showed that innovation in the United States is generally strong. “Linking National Security and Innovation: Part 1” provided an overview of the relationship between national security and innovation now that the DOD has gone from being a producer to a consumer of innovation.

“Mapping the National Security Industrial Base: Policy Shaping Issues” looked at how today’s commercially driven innovation ecosystem differs from earlier national security innovation ecosystems. It found that while the United States is not lagging in innovation, the national security community needs to adopt new approaches for investing in and acquiring innovative commercial technologies. Both reports found that the challenges for national security innovation lie in how to change investment and acquisitions processes that were designed to minimize risk, something that many other reports have highlighted. This study makes a series of recommendations for funding, process, and culture.

The goal is to find new ways to connect national security to a risk-taking, entrepreneurial culture that is skilled at turning research into commercial products. For the federal government, a risk-averse culture and underfunding are the primary impediments. The fundamental conclusion of this report is that efforts to modify the current system to make it more “innovation-friendly” will not work without strong congressional mandates. To acquire innovative technologies, the United States needs new approaches to create alternatives in funding and organizations for acquiring technology. New approaches mean redirecting funding and creating alternatives to existing technology acquisitions processes.

¹ This is a misnomer, since innovation has become transnational, but this paper will look at a national innovation system with significant transnational elements.
PROVIDING SUFFICIENT FUNDING

The private sector now leads in innovation and accounts for around 75 percent of U.S. R&D spending, but most innovative companies are interested in commercial markets, not defense. National security does not offer the scale of financial returns they want, and they have reasonable concerns about regulation, bureaucracy, and compliance burdens that deter entry into the market.

The national security community recognizes this dilemma and is beginning to make changes—under the direction of Congress—in how the DOD develops and acquires technology for national security purposes. First, the national security community, in response to the fundamental changes in the innovation ecosystem, created new organizations, such as AFWERX or DIU. There are now perhaps 30 such “nontraditional” organizations across the national security community. Despite the increase in the number of organizations focused on innovation, they remain underfunded compared to the private sector or the traditional defense-industrial base.

Comparing different industry sectors provides a sense of the scale of underfunding. Overall, 3 percent of U.S. national income is spent on R&D (mainly for the development of new products and services), but this percentage varies widely by sector. Companies in healthcare and information technology spend the most—on average a little more than 20 percent of their total revenue goes to R&D. In contrast, the telecommunications sector, which spends the least, dedicates about 1.6 percent of total revenue to R&D. Defense and aerospace companies spend more on average, about 2.9 percent. It is safe to say that every major sector except telecommunications spends a greater share of revenue than the DOD when it comes to innovation. Even though there has been much work on acquisition reform, there has not been much of a shift from large defense primes to nontraditional vendors when looking at DOD spending.

Innovation consists of the R&D needed to bring new products and services to market, and for the national security community, nontraditional innovation means drawing upon the companies and start-ups that do not currently work with the DOD. This report uses a focused definition of innovation—the development and acquisition of commercial technology to national security problems—and counted programs that are closest to innovation in a “Silicon Valley” entrepreneurial sense. Using this definition, in FY 2020, the DOD devoted just 0.055 percent of its budget to nontraditional innovation.

If this is expanded to include the Defense Advanced Research Projects Agency (DARPA), perhaps the premier defense research organization in the world, the number improves. Including DARPA, the DOD devotes 1.49 percent of its acquisitions budget to innovation. If the DOD was a company, its budget would put it in the top 10 of the Fortune 500. Total defense spending by the DOD on R&D in 2021 is $30 billion; this is less than Amazon ($43 billion) and slightly more that Alphabet ($28 billion). Both Amazon and Alphabet spend a greater percentage of their revenues on research than the DOD. The five biggest spenders in the tech sector spent a combined total of $125 billion on R&D.

_Innovation consists of the R&D needed to bring new products and services to market, and for the national security community, nontraditional innovation means drawing upon the companies and start-ups that do not currently work with the DOD._

An imperfect comparison with a business is that while “income”—the amount appropriated by Congress every year—is high, “net revenue” is much smaller when other costs are deducted. The DOD must sustain
a huge force and invest billions in new conventional weapons platforms. Spending on acquisitions (as opposed to maintenance and operations) reached $365 billion in 2020. An initial recommendation is to spend more on nontraditional innovation by setting a numerical target for funding and directing that this funding can be used to support nontraditional organizations.

An April 2021 CSIS publication, *How Much is Enough?*, estimated that the U.S. government needs to spend $250–300 billion if it is to compete with China and maintain its leadership in technology. This seems like a lot, but the United States is in a conflict with China (China’s leader believes this). U.S. spending on R&D was consistently strong from 1958 to 1990 during the confrontation with the former Soviet Union. R&D investment was seen as integral to the national defense. The same is true now. After underinvesting for decades, the United States will need to commit to continuous funding for a period of years. But the return on investment and the likelihood of success could be increased if the United States improves its ability to acquire innovation for national security purposes. Informal estimates suggest spending on nontraditional innovation should be increased tenfold.

Funding provides an indicator of seriousness and intent. Nontraditional innovation programs receive less than 1 percent of acquisitions funding. Congress can change that by increasing funding for nontraditional efforts. Budget increases will go far to remedy this problem when they are both authorized and appropriated.

**BUILDING THE RIGHT CULTURE**

Even with increased funding, the national security community will not get the full return on its investment because innovation requires more than R&D, as valuable as it is. It also requires entrepreneurship, or the willingness of individuals to take on higher-than-average risks. It is the combination of innovation and entrepreneurship that has made the United States so successful in creating new technologies. This is to a degree antithetical to how things currently work for national security. Many analysts have noted that the national security community is risk averse. Finding ways to create an increased tolerance for risk is a broadly accepted goal for strengthening the national security community’s ability to acquire innovative new technologies.

The problem with this is that after more than a decade of trying to change culture, the United States has made slow progress. Most recommendations to change culture will take years to accomplish, requiring time it does not have. Thomas Kuhn’s seminal work *The Structure of Scientific Revolutions* described how ideas change. Why refer to a book from the 1960s to describe today’s national security innovation problems? Kuhn concluded that the holders of old ideas do not change their minds, but that new actors and ideas emerge. This means that connecting the national innovation system to national security problems requires creating these new actors in the form of new organizations.

The current system excels at doing what it was designed for: ensuring the DOD has what it needs to operate and build major weapons systems, such as aircraft carriers or fighter aircraft, depending upon the current U.S. military doctrine. In this environment, a steady, risk-averse approach can be best. However, this is not the way to acquire commercial innovation. As a recent Senate Armed Services Committee chairman said, “the Pentagon has often proven an impossible customer due to its antiquated bureaucracy.” The current acquisitions system leads entrepreneurs and investors to avoid the national security community as a customer. Other concerns also reduce participation. Some tech entrepreneurs worry that building for defense risks having their product “export controlled,” putting bureaucratic hurdles in front of access to global markets. Nor does the national security market always offer the scalability that entrepreneurs and investors want when compared to a global commercial market measured in the trillions of dollars.
The investment and acquisitions system has deep and valuable ties to the defense-industrial base. It does not have the same ties to the national innovation base. Instead of reengineering the existing acquisitions establishment, the DOD should create new ones to complement it. While there have been efforts in recent National Defense Authorization Acts to improve the DOD’s ability to acquire technology from the private innovation system, Congress and the national security community should complement efforts to make the existing defense acquisitions more innovation-friendly with similar efforts to authorize and fund new national security innovation actors. This two-track approach will allow for the long-term changes considered necessary and provide an immediate improvement in the ability to identify and develop innovative technological solutions to national security problems.

The United States can build upon small, nimbler, nontraditional organizations, like AFWERX, DIU (and the National Security Innovation Network), Army Futures Command, NavalX, and SOFWerx. While all differ in varying degrees in their missions and authorities, they offer the elements of a new and separate approach to acquiring innovation. Trying to embed these innovation organizations into the existing acquisitions structure in hopes of creating cultural change risks diluting (or submerging) any new approach. As funding levels show, these are currently more similar to add-ons to the existing acquisition’s structure rather than outright alternatives. Congress may need to modify or expand existing authorities to create an alternative institutional framework for innovation.

**DEVELOPING ADEQUATE PROCESSES AND AUTHORITIES**

In 2015, Secretary of Defense Ash Carter sought to expand the connections between the national security community and Silicon Valley. There has been progress since, but it has been an uphill struggle; as funding numbers show, the United States still has twentieth-century acquisitions systems developed to acquire technology from a twentieth-century innovation base. Changing this requires both short-term fixes that use existing authorities and a longer-term reorientation if the United States is to outperform its opponents.

The national security community has the ingredients needed for a new approach to acquiring innovation: the size of its budget, skilled human capital, and unique authorities. Accomplishing this will require modifying some processes and authorities, expanding others, and, in some instances, creating new ones. There are necessary steps beyond increased funding. The areas where change is needed include providing the authority to cooperate with trusted foreign partners, allowing alternatives to POM budgeting, allowing innovative organizations to acquire equity in start-ups, setting mandatory percentages for spending, and rebuilding a tech assessment capability.

*The United States still has twentieth-century acquisitions systems developed to acquire technology from a twentieth-century innovation base. Changing this requires both short-term fixes that use existing authorities and a longer-term reorientation if the United States is to outperform its opponents.*

**Assessment**

As a first step, the national security community needs to rebuild its technology assessment capabilities. Mapping national security needs to the innovation base is difficult because the DOD may not always be aware of what is available on the market, and many of the assessment processes developed for the Cold War have been dismantled or fractured and may not be appropriate for a technology innovation system.
centered on work in the private sector. An integrated assessment process would be able to identify national capabilities, allied capabilities, opponents, and the status of their innovation systems. This could be a new senior government council or an expanded mission for an existing senior group. These efforts should be accompanied by a continuing expansion of U.S. intelligence community efforts to assess foreign capabilities. There will also be a need to include domestic agencies, which suggests a leadership role for the White House in coordinating defense, intelligence, and domestic assessment capabilities.

Given existing constraints, the U.S. intelligence community is limited in its ability to assess U.S. companies, but the same constraints do not apply to civilian agencies. The Department of Commerce has authorities under the Defense Production Act that allow it to survey industry sectors. It currently has offices scattered among its bureaus that have assessment capabilities. The Department of Commerce may need to reconstruct its “Technology Administration” bureau to provide a central point for such assessments.

**Greater Use of Existing Authorities**

Despite repeated congressional mandates, the national security community has been reluctant to use its existing authorities to acquire new technologies. This reflects problems of inadequate funding and a risk-averse culture. A lack of congressional oversight also contributes to the unwillingness to depart from FAR-based contracting. A first step is to make greater use of existing authorities for acquiring innovations. The two most important of these existing authorities are found in FAR Part 12 (the acquisition of commercial items and commercial “off-the-shelf” items) and the use of the OTA. These offer faster, more flexible ways to invest in and acquire innovative technologies. The temptation, particularly as the use of OTAs grows, is to subject these to FAR-like requirements for compliance, which will defeat the purpose of accelerated processes.

**Program Objective Memorandum Alternatives**

One thing the U.S. government can learn from commercial practices is the importance of speed. The national security community needs to increase the pace of acquiring new technology. Existing processes will not allow for this. POM’s multi-year planning process increases the risk that the technology acquired under it will be out of date when it arrives in the field. The template for progress toward the goal of tapping into the innovation ecosystem is to copy the private sector, particularly VC. The United States needs to use alternatives to the POM process.

This means committing to faster timelines and greater flexibility to commit funds. There is no real way to sync innovation and a two-year POM process. Innovative organizations should have discretionary funding to invest and own equity in start-ups to better partner with private sector investors and entrepreneurs. Speeding up the current two-year budgeting process will help the DOD adopt innovative technologies while leveraging various contracting authorities. One approach is to expand the use of efforts such as the Commercial Solutions Opening pioneered by DII. This allows companies to compete and prove their technology’s usefulness as a military application and then move quickly to a production award. Speeding up the current two-year budgeting process will help the DOD adopt innovative technologies while leveraging various contracting authorities.

**Foreign Participation**

No private company or investor interested in innovation would limit itself to U.S.-owned companies. Congress and the Biden administration need to provide the authority to cooperate with trusted foreign partners. The Small Business Innovation Research (SBIR) program, for example, requires that the companies it supports be “primarily U.S. owned.” Legislation that authorizes the “National Technology and Industrial Base,” which allows for cooperation in R&D and production in the United States, Canada, the United King-
dom, and Australia, does not fit well with the new innovation ecosystem. As part of the larger effort to develop cooperative joint approaches with allies to develop and acquire technology, this requirement should be removed. Companies in trusted partner countries should be allowed to bid, compete, and win contracts.

A nontraditional approach to innovation would benefit from the United States bringing in trusted partners, starting with close allies. There are many proposals for this, and the easiest place to start might be with the Five Eyes partners, which have strengths in different technologies and with whom there are records of cooperation on national security–related technologies. Involving trusted partners would make the most sense if it was part of a larger, coordinated national innovation strategy. This is well underway in the current administration and Congress, with the U.S. Innovation and Competition Act and its components, the executive branch attention to technology and innovation, and the creation of the Trade and Technology Council with the European Union.

**Mandatory Budget Requirements**

It has proven difficult to change culture, and one of the techniques recommended to achieve this is to create incentives. The best incentives would be to tie the allocation and disbursement of conventional funding to funds for innovation. Funding set-asides for investment as some mandatory share of the total acquisitions budget would ensure greater support for innovation. This level should begin at 3 percent of the acquisitions budget and include funding to expand staff at nontraditional organizations.

**INNOVATION NEEDS A CONGRESSIONAL MANDATE**

The POM process often leads the national security community to end up creating “bespoke” technologies for which there are already commercial solutions. One reason for this is that skill in managing the POM process is more important than innovating.

Some have even proposed that “commercial buying should be the default rule for new R&D and production programs in select areas.” This sounds draconian, but it is probably necessary. The best way to achieve change is to mandate funds that can only be spent using these authorities. This is important because there are instances where some national security agencies have ignored commercial tech options to commission “bespoke” software, often at higher prices.

**Authorize the Acquisition of Equity**

VC firms will fund start-ups or early-stage companies that offer technologies with innovative national security applications. VC firms invest in these companies in exchange for equity, which means taking an ownership stake in the company. This comes with some risk: a VC equity investment is basically a bet on a company and its technology. This acceptance of risk drives innovation in the United States. Federal innovator organizations should be allowed to invest and own equity in start-ups to better partner with private sector investors and entrepreneurs. Congress and the DOD have begun to allow for some equity acquisitions, but only on a small scale. The National Security Innovation Capital (NSIC) has only $15 million in funding. NSIC and related efforts are best seen as proof-of-concept initiatives which show that the United States could benefit if it increased funding for nontraditional agencies as well as their ability to obtain equity.

**In-Q-Tel**

One possible expansion of an equity-acquiring approach would be to either create more organizations like In-Q-Tel or give existing organizations authorities similar to In-Q-Tel. In-Q-Tel is unique, like a VC firm. In-Q-Tel is government funded but privately operated without direction from its sponsor. It can invest in and hold equity positions, retain the title to innovations, and share in revenues in the start-ups it supports.
in ways that DOD innovators cannot. The CIA, which created and sponsors In-Q-Tel, only retains “government purpose rights” to any innovation. This makes it easier to work with start-up firms and with VC firms. Giving AFWERX, DIU, and others the authority and funding to hold equity in start-ups of interest and to act generally like angel investors or VC firms would strengthen the national security community’s ability to acquire innovative technologies. This recommendation can make some uncomfortable, but greater independence in operations and the authorities allowing nontraditional organizations to act more like VCs would help compensate for risk aversion.

**Streamline Compliance**

Streamlining compliance processes is crucial for innovation. The FAR, for example, has more than 2,000 pages of rules, and some estimates put it at over 4,000 pages. The companies that succeed in this environment are often those that are best at managing complex acquisition paperwork. Just as there are organizational alternatives to the conventional system, there are alternatives to FAR and DFAR (Defense Federal Acquisition Regulations) contracting.

There are fears that simplifying investment processes for acquiring innovations could weaken oversight. This assumes however, that the current level of oversight and compliance (which represents an accretion of rules over decades) is necessary. The experience of the nontraditional entities shows that a more minimal approach to oversight is sufficient rather than excessive. Speed and agility are among the defining characteristics of private sector innovation and should be the benchmark for national security community efforts. Concerns about oversight should not become an obstacle to gaining access to a vendor base many times larger than the traditional base used today.

**Speed and agility are among the defining characteristics of private sector innovation and should be the benchmark for national security community efforts.**

**A NEED FOR LEGISLATION**

In-Q-Tel may not be the perfect model, but it provides useful lessons. Rather than reworking the FAR system, Congress could create new legislation providing for an alternative to FAR-based acquisitions. The goal of the legislation should be to duplicate how private sector investment and acquisitions of innovation work. Any potential new legislation should emphasize the principles of speed, funding, and flexibility:

- Create an assessment capability to identify new technologies of interest.
- Mandate organizational changes to reinforce links between nontraditional organizations and the services and program offices.
- Fund investment in nontraditional sources of innovation at some mandatory share of the total acquisitions budget. This level should begin with 3 percent of the acquisitions budget and include funding to expand staff.
- Create a separate budgeting process for nontraditional organizations that breaks out of the current two-year POM cycle. This is an area where China can gain an advantage with its more flexible processes.
- Authorize nontraditional organizations to hold equity positions in start-ups.
QUESTIONS THAT NEED ANSWERS
The recommendations of this report are to increase funding from nontraditional innovation, create alternative organizations focused on nontraditional innovation, and either ensure that they can make full use of existing authorities or provide new authorities that enable them to act more like VCs. Doing all this would accelerate the acquisition of new technology by the national security community and improve the United States’ ability to compete with China.

However, this would still leave a number of open questions. The first is the degree to which funding for nontraditional innovations could be made mandatory, perhaps by having Congress set a numeric threshold. This would be unusual but may be necessary given the reticence to fund new approaches to acquiring innovation. Congress might also consider requiring greater use of FAR Part 12 authorities for acquisitions of products and services that are already available. In theory, the government is not supposed to make its own products when a commercial alternative is available, but this is not always observed in practice.

The increasing number of nontraditional organizations for tech acquisitions does limit the ability to coordinate (except in an ad hoc fashion), but since most nontraditional organizations are created by and dedicated to one of the services and focused on their needs, this problem may be smaller than it appears. Consolidation of the few agency-wide programs, such as SBIR, could increase efficiency and return on investment.

In theory, the government is not supposed to make its own products when a commercial alternative is available, but this is not always observed in practice.

A second issue is organizational: Should the United States seek to consolidate the many nontraditional organizations under a single entity? There are still gaps between nontraditional innovation organizations and program offices. Remediating this will require training to understand the business model of innovation. A greater degree of centralization could provide greater direction and might help remedy this. Greater clarity may be possible by giving DIU a more directive role in the SBIR/STTR (Small Business Technology Transfer) process. However, given the close relations of the nontraditional organizations to specific services (e.g., AFWERX to the Air Force, NavalX to the Navy) and the benefits of organization discussion for innovation, consolidation may be of limited value.

CONGRESS IS CRITICAL TO MOVING FORWARD
Innovation can be hard to measure. In this case, there are simple metrics for success in linking the national innovation system to national security, such as measuring how much funding has gone to nontraditional vendors and how many projects have successfully transitioned to production contracts. The benefit of these two metrics is that they are numeric, uncomplicated, and accurate.

The imperative for change should be clear. The United States is in an era of competition with powerful authoritarian states that intend to reorder the world to better suit their interests and values. Russia and China, the United States’ major competitors, are formidable technological powers, especially China, with its size and wealth (and its heavy-handed technological espionage). The United States’ comparative military advantage in technology has eroded. The wars in the Middle East sapped resources and attention; China has accelerated its efforts to gain technological leadership; and commercial technologies increa-
ingly provide military advances. New commercial technologies will provide dominance in future wars, and while the United States is well placed in the innovation race, maintaining its technological advantage in national security will require new approaches to capturing commercial innovation.

The need to change funding, culture, processes, and authorities all leads back to Capitol Hill. If the United States is to make the national security community more “innovation friendly,” it will in most cases require congressional action and oversight. While most in Congress are supportive of accelerating innovation in the United States and increasing funding, the main obstacle when it comes to the national security community is the accumulation of oversight processes designed for major weapons programs. Streamlining will not occur naturally—it requires congressional direction. How the United States creates innovative technologies has changed, and Congress can use its authorizing and appropriations responsibilities to ensure that the national security community changes with it. A mix of new funding priorities, mandates that emphasize acquiring commercial technology, and supportive authorities for nontraditional organization can move the country along the path identified years ago to harness the powerful U.S. private sector innovation engine for national security.

*James Andrew Lewis* is a senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C.

This report is made possible by support from the Department of Defense.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2021 by the Center for Strategic and International Studies. All rights reserved.