APRIL 2021

Linking National Security and Innovation: Part 1

By James Andrew Lewis

The Department of Defense (DOD) has gone from being a producer to a consumer of innovation. Innovation occurs outside of the defense economy, and America needs new ways to link innovation to national security, given both aggressive competitors and the U.S. policy mistakes of the last 20 years. Essentially, the United States does not spend enough on national security research (compared to spending in earlier contests), and DOD procurement processes, designed for major weapons systems acquisitions, are an obstacle to innovation. These are daunting problems, but there are solutions and a growing willingness in Congress and the policy community to apply those solutions.

Americans know that China has decided to compete with America in technology—part of a larger strategy to replace the United States as a global leader. The United States, in response, has decided to strengthen its own technological base. This is the fourth time the United States has pursued technological leadership to answer a strategic challenge. The foundation of the strong link between technology, science, and security was laid in World War II. The response to Sputnik created a huge and foundational national effort for American technology. In the 1970s, the contest with the Soviets again drove innovation. Each episode required increased spending, but this paid for itself by creating powerful industries that drove American economic growth.

The United States can draw lessons for this new conflict from the last great challenge. In the 1970s, William Perry, then the undersecretary for acquisitions, committed DOD research efforts to technologies that would overcome or offset the Soviet numerical advantage in weaponry. His investments in precision guidance, stealth, sensors, and communications created what many called a "revolution in military affairs" that proved decisively superior in the 1990 war with Iraq. Technology gave America unquestioned military superiority for three decades, but this unquestioned lead has ended. The task now is to restore it.

Maintaining U.S. technological leadership is a good policy objective. But after every war, America cuts defense spending, and the Cold War was no exception. There were significant cuts in support for research and development (R&D). The one exception was funding for the National Institutes of Health. Congress increased spending on life science R&D, but it then trimmed the "hard" sciences (e.g., physics, math, and materials). Government funding is essential for fundamental research in these areas—research that by

itself has no immediate commercial value but creates the basis for commercially valuable innovations and for military strength.

The Endless Frontiers Act, when it is funded, will begin to remedy these 1990s cuts. This is a good start for repeating earlier successes in using technology to advance national security. However, there are now crucial differences in how America creates new technologies that require a new approach. America's national innovation base has changed dramatically in the last three decades. While defense prime contractors remain engineering and technological powerhouses, they are not the source of innovation. Similarly, the centralized private labs such as Bell Labs or Xerox Parc that played a major innovative role in the last century no longer exist. These changes do not mean U.S. innovation is weak, but that it is different. U.S. innovation is strong, and major technology companies invest heavily in R&D, but it is focused on "D"—the development of new products and services for commercial markets. The transformation in how America creates new technology has altered the relationship between national security and innovation.

This transformation in the nature of innovation in the United States is the result of several factors. First and most important is the central place technology now occupies in economic activity. As one bank CEO put it, "every [big] company is now a technology company." Private sector investments dominate R&D for new technologies, in 5G, artificial intelligence (AI), biotechnology, quantum computing, and alternative power sources. Second, innovation shifted to the private sector as a result of flat federal spending on R&D. This helped incentivize a focus on commercial markets. Finally, post-Cold War peace brought a wave of global business opportunities that dwarfed the national security market. These three factors mean that most innovation now occurs in the private sector and is focused on commercial developments.

Also, while the Cold War innovation base was largely national, today's innovation base is international, with linkages between the United States, Europe, and Asia. AI is a good example, with strong research centers in the United States, United Kingdom, Canada, Germany, Israel, and China, and a significant degree of cross-fertilization among them. Efforts at "reshoring" will not change this. While these interconnections can create security risk when it comes to technology transfer, the benefits they create outweigh any risk, and any country that cuts itself off from this international innovation system will fall behind.

This makes the task for the United States needs to expand the role of innovation in national security to find ways to take advantage of a multinational commercial innovation base. The U.S. government does not have the financial heft to shift back to a "government-centric" innovation base, but focused investments and revised authorities can recreate the link between national security and innovation.

Linking Innovation to National Security

Until the 1990s, the DOD played a major role in innovation as investor and first adopter, with its contracting power and ability to direct research, but there has been a significant change driven by the immensely expanded commercial market for technology. The center of gravity for innovation and tech investment has moved away from government. Entrepreneurs and tech companies would rather chase this profitable commercial market than develop technology for the DOD. The scale of returns from the commercial market dwarfs the defense market, and the barriers to entry to the national security market can be prohibitive.

Simply trying to recreate the DOD-centric approach of the Cold War era will not work in the new innovation environment. Nor should the United States copy China's government-driven approach to investment. Even Beijing recognizes how political goals can warp its investment strategies as party functionaries scurry to implement the latest mandate.

The shift to private-sector-led innovation and the decision of firms to focus on commercial innovation rather than national security make economic sense, but they create two problems for national security. The first is that private investment in fundamental research can fall short, weakening the national innovation base. Government investment in this area is required. The second problem is the lack of efficient mechanisms to identify and acquire innovative technologies from the commercial sector that can advance national security. Acquiring innovation, which often occurs in small, entrepreneurial firms outside the traditional defense industrial base, may require taking a page from how venture capital (VC) firms use a deep knowledge of a technology sector and close networking with the tech community to identify investment opportunities.

There are fears that companies will not want to work with the DOD for ideological reasons. This may be true for a few, but the reluctance of startups to work with the DOD has more to do with incentives. Government funding is limited, and DOD procurement is cumbersome and complex. Change the incentives, and innovators will come.

If the goal is the development of more innovative technologies, funding should be shifted. The targets of investment in innovation will fall largely outside of the traditional defense industrial base. Raj Shah, the first director of the Defense Innovation Unit (DIU), noted that the DIU's budget is a "rounding error" in the context of DOD spending. He recommended a tenfold increase. The DIU was created by former secretary of defense Ashton Carter to help improve DOD access to innovation and has since been copied by other DOD entities, such as AFWERX. The DIU, for example, has worked with more than 100 vendors who do not usually bid on defense contracts, including many who had never before worked with the DOD. While these efforts have been markedly successful, their funding needs to be scaled up significantly. This does not mean there is no role for the existing defense industrial base, but the best strategy for those firms may be to mimic the tactics used by tech giants—to acknowledge that they are no longer innovation leaders and instead focus on identifying and acquiring innovative new startups to stay on the cutting edge.

Should the United States Copy China?

China's decision to build a strong technology base for defense goes back to Chinese leader Deng Xiaoping in the 1980s. Starting with Deng, China developed a three-pronged approach, using large investments in research and technology firms, spending to build a skilled workforce (often by funding Chinese students to study at Western universities), and engaging in technological espionage. China copied the defense innovation model used by the United States in the 1970s and 1980s, but its approach is also shaped by its experience with Soviet-style planning. The heyday of Chinese innovation occurred before the current leader, Xi Jinping, began imposing greater political controls, requiring greater conformity, and re-emphasizing state-owned enterprises rather than private companies. The effect of these decisions is not yet fully known, but they could hamper innovation in China. Chinese policy is to pursue "Military-Civil Fusion," where the government plays a more directive role. Military-civil fusion is probably a bad idea (party officials are not the best source of investment advice), and we have yet to see how Xi's political tightening affects Chinese innovation capabilities. But China's pool of human talent and its commitment to workforce-building and government investments give it an advantage. The United States can match workforce and investment but has so far chosen not to do so.

The National Innovation System

The U.S. innovation system remains the envy of the world, with its blend of strong research universities, flexible financial systems, and a fast-moving, risk-taking, entrepreneurial business culture. Many other countries have similar strengths, but usually not in all areas, even in China, and not at the scale of the

United States. The United States should not lose sight of this strength. Its chief problem is how to better connect America's strong innovative system to national security.

The innovation process turns research into products and services. A simple model of the innovation system would include three classes of participants: researchers to come up with new ideas, financiers willing to take risk and invest in new companies and technologies, and entrepreneurs who turn research into products.

This model would include researchers at universities or corporate labs, who are often funded to look at a specific problem at the request of companies or government agencies. It includes a risk-taking entrepreneurial community (sometimes university professors or their students who see the opportunities of their research) that understands how to connect research to markets. It includes financial actors, such as an aggressive VC industry and other financial entities, including the VC arms of major companies, which invest in new technologies, entrepreneurs, and startups. VCs and startups are at the core of this innovation system. There are more than 1,000 VC firms in the United States (most still clustered in California, Massachusetts, and New York), with more than $130 billion invested$130 billion invested in roughly 10,000 companies (in 2019).

Reconnecting national security and innovation means investing in small, entrepreneurial firms that are outside of the traditional defense industrial base. The national innovation system has an intensely commercial focus. Entrepreneurs and investors want to make money. They are drawn to the areas that promise the best returns. This is often not the defense market.

One drawback to this focus on returns is that many innovative firms focus on software products and services. Demand and returns for these "intangible" goods are high, and barriers to entry are low. In some areas, such as AI, this focus is helpful. But the hope of being the next Spotify or Google (or being bought by Spotify or Google) can disincentivize developmental work on manufacturing or hardware that might be of value to national security. Targeted federal spending, particularly in areas where commercial and national security interests overlap, can change the incentive structure to overcome this.

One thing to note is that the national innovation system is an incremental, distributed process. It is not linear. Tangled connections are the norm in VCs, since a deep knowledge of the industry is essential. Serendipity plays an important role when research in one area turns up something of use for another problem. Many firms and institutions are involved, with researchers and entrepreneurs building upon and expanding the work of others (this is one reason that patents and intellectual property protections are important for innovation). One benefit of an incremental and distributed process is that it provides more opportunities for the DOD to insert itself into the innovation process if it can identify these opportunities and if it has the authorities and funding to take advantage of them. However, it also reduces the value of any top-down approach to innovation.

Mapping national security needs to the innovation base is difficult because commercial incentives and national security needs will not always align. The DOD may not always be aware of what is available on the market. This is where expanding the entrepreneurial approach seen in the DIU, AFWERX, and others would be useful to be able to identify, invest in, and "harvest" commercial technology. The DOD may be better served in gaining access to innovation if it identifies or modifies commercial technologies for national security purposes rather than pursuing "custom-made" technologies. The private sector is going to outspend the DOD in key areas. Commercial space programs are an example of private-sector leadership, as is quantum computing. One lesson in both fields is that it can be more efficient for the DOD to buy and modify commercial products or to create incentives for private investment to expand and reinforce its spending, rather than for the DOD to build its own.

Does the DOD Need to Make "Big Bets" on Technology?

Some in the national security community hope to replicate William Perry's 1970s strategy by making "big bets" on a few technologies to restore American military advantage in technology. Trying to replicate Perry's success makes sense for some areas, such as identifying mission areas that will benefit from advances in AI, unmanned vehicles, networking, sensors, space, and communications. But "big bets" is a 1970s strategy. That alone should give pause. The greatest risk is that the DOD will make "big bets" on the wrong technologies or the wrong firms. Solyndra, a targeted technology investment, is a cautionary tale. Since many innovative technologies are still in an early phase, it is too early to make big bets.

This is a question of investment strategy. Does the government select a few technologies and concentrate a few big bets on them, or should it take a distributed approach, with many smaller bets on multiple innovators and technologies? This portfolio approach is how innovation works now since it reduces the risk of making the wrong choices. The DOD might be better served by defining mission areas that could benefit from innovative technologies and then creating the incentives for entrepreneurs to develop them.

In conventional acquisitions, the DOD or a military service identifies a need, develops requirements, receives proposals to meet those requirements, and awards a contract. This is a linear (and lengthy) process designed to reduce risk. Big bets make sense for this model, but it is not the best way to use the national innovation system today. To use quantum computing as an example, it is too early to make a "big bet" on a technology that is still in development that the private sector already spends heavily on, and whose use will significantly reshape key technology areas. If there is a big bet for quantum, it is to expand support for private sector and academic R&D. Many small bets are better than a few big bets in an uncertain and changing environment.

Is In-Q-Tel a Good Model?

In-Q-Tel is the CIA's investment arm modeled on VC firms. The CIA faced the same problem as the DOD—its acquisition processes kept it from accessing cutting-edge technology and from using that technology to address operations problems. In-Q-Tel has been a success, and its flexible authorities are a good precedent for the DOD, but it acts more like a conventional VC firm. In-Q-Tel and the DIU often invest in the same technology areas, but the authorities they operate under are very different. The DIU and other DOD innovation groups are DOD organizations. In-Q-Tel is a stand-alone, non-profit corporation. These differences mean there are limits to In-Q-Tel as a model for the DOD.

Making National Security an Innovation System Focus

There is now general recognition of a "disconnect" between the DOD and innovation centers such as Silicon Valley. Some of this is because, to quote former SASC chairman Jim Inhofe, "the Pentagon has often proven an impossible customer due to its antiquated bureaucracy." Equally important, DOD acquisitions do not offer the market scalability that entrepreneurs and VCs hope to gain because the DOD is not in a position to compete with the multi-trillion-dollar global commercial market for technology. Market forces alone will not fund products intended for the defense market. Nor does the disparity in market sizes mean that the DOD can expect to redirect most private investment to meet its needs. As the market for advanced technology has spread beyond the DOD, it is no longer the "anchor tenant" in the national innovation system.

While one congressional leader called for a "wholesale change to industry culture" to prioritize national security, the opposite is true. The DOD is the one that needs to change its culture to accommodate and leverage the national innovation base as it exists now.

But the DOD has advantages, and these create opportunities. Tailored and targeted spending programs, use of DOD authorities and abilities to provide testbeds and prototyping, and the attraction of working with the Defense Advanced Research Projects Agency (DARPA) and other DOD research centers will draw companies. Working on difficult tech problems of national security interest (not found in the commercial space) can lead to new commercial opportunities—think of the internet, which began as a DOD research project. All of these factors give the DOD the potential to expand its access to the private sector national innovation system.

Congress has used the National Defense Authorization Act (NDAA) to bolster the DOD's ability to acquire new technologies. This includes support for the traditional defense industrial base but also the broader network of startups and other firms that make up the national innovation system, which is more likely to be the source of future innovations. Adding support for this "alternative" innovation base is a good idea since the most important obstacle to national security innovation after insufficient funding is DOD regulation and culture. The pace of innovation is fast, but this entails risk. Entrepreneurs do not want to spend weeks filling out forms and then have to wait months for a decision. In the VC world, deals can be done in a matter of weeks. Complexity and delay have been disincentives to working with the DOD.

An example from a few years ago comes from a startup working on cutting-edge, AI-driven sensor technology valuable for unmanned aerial vehicles. The entrepreneur-owner approached the Pentagon, was given a sheaf of forms, and was told to fill them out and come back in a few months. By coincidence, a Chinese investor approached him at the same time and offered to write a check for $10 million on the spot. Fortunately for the United States, the entrepreneur declined the offer and went with the DOD, but the comparison is startling and indicative. Others might have exited the defense market.

The 2018 *National Defense Strategy* put it like this: "The current bureaucratic approach, centered on exacting thoroughness and minimizing risk above all else, is proving to be increasingly unresponsive." Complexity and a deliberate pace make sense in the world of multi-million- or multi-billion-dollar weapons acquisitions programs, but they are obstacles to innovation and impediments to the participation of smaller, innovative firms in the national security innovation base. The DOD acquisition process focuses on structured program execution that minimizes risk. Innovative startups, however, embrace risk, and risk is central to innovation.

One solution has been to use Other Transactions Authority (OTA). OTA creates contractual instruments for research and prototyping activities. OTA is not subject to the regulations that govern conventional procurement contracts. There are fewer than 100 pages of guidance for OTA, compared to almost 4,800 pages for standard acquisition policy, regulation, and best practices. But OTA makes up only a small fraction of DOD acquisitions spending. Concerns that OTA somehow circumvents oversight procedures are not born out by experience. Any additional risk is justified by the urgent need to bring innovation to national security for an increasingly confrontational world with opponents who aggressively pursue technological superiority.

Congress's Opportunity

The task of changing the acquisition system to accommodate innovation and entrepreneurship falls first on Congress since what it needs is more funding and new authorities. There have been significant legislative efforts in the last few years to do this, most recently in the House and Senate NDAA bills that focus on promoting and acquiring innovations and technology from the private sector entities that make up the national security innovation base.

To continue and build on this trend, Congress needs to adequately fund the national security innovation base and give DOD organizations the authorities needed to operate more flexibly and in ways similar to commercial best practices. This can be done best by reweighting funding priorities, adjusting rules and cultures to accept more risk, and gaining senior leadership support for alternate vehicles and policy.

Increased funding is critical. This includes both fundamental research funding as well as increased resources for non-traditional acquisitions and investments. The bulk of DOD spending still goes to twentieth-century platforms made by the conventional defense industrial base. To remain competitive, the share of funding for the national security innovation base should increase. Increased funding will change the incentive structure for entrepreneurs and innovators as they make business decisions on where to spend their time and energy. To put this in perspective, not only is China closing the funding gap, but the United States now spends significantly less than it did at the height of the Cold War.

Measures to strengthen the national security innovation base can be kept separate from efforts at acquisitions reform. The DOD needs to manage thousands of contracts worth billions of dollars, and this is a different task than accessing innovation. Acquisitions culture will not change overnight. There is a complex system of oversight and rules that will be difficult to amend. Innovation is best accelerated in a smaller, parallel stream of activity and with new organizations that have a different attitude towards risk. Ultimately, there can be greater integration of the two streams, but this will take time. An alternative acquisition structure more attuned to technological innovation has emerged with the creation of smaller organizational entities such as AFWERX and the DIU. The success of these new organizations points to a series of actions necessary in the next NDAA:

- **Fund:** Provide more funding for the national security innovation base. Federal spending underpins fundamental research and is critical for attracting entrepreneurs.
- **Streamline:** Identify where legislation can expand incentives or remove obstacles for innovative companies to participate in national security innovation. This may involve reinforcing and clarifying authorities for the national security innovation base to allow more flexible approaches, including more risk-tolerant acquisitions and funding processes that make it easier to turn R&D into deployable technology. VCs can provide a partial model for this.
- **Connect:** Link the national security innovation base to progress in developing a new "industrial policy" for the United States. This is still being defined in policy and law but has innovation and technological leadership at its core.

Next Steps

The United States would not be having this discussion if it were not for China. The United States is challenged by a powerful and hostile state actor. Technology has become one of the principle battlefields, and there are concerns that the low-budget, laissez-faire approach of the last three decades is inadequate. In fact, the United States is doing well in most emerging technologies, but there are reasonable concerns that this reflects investments made in the past that have not been replenished and that the United States is not moving quickly enough to stay ahead of China.

Paul Kennedy's book *The Rise and Fall of the British Navy* ended by noting that big powers fail because they keep doing what worked well in the past even when it no longer works. Technological leadership has been at the core of U.S. national security for decades, but the United States faces intense competition, and important changes in America's innovation ecosystem have created new requirements for continued leader-

ship. The next phase of this project will map and define the national security innovation base. The third report in this series will describe how to change the incentive structure to strengthen the national security innovation base. It will look at commercial best practices, determine where national security innovations fit into new approaches being considered in Congress and the Biden administration on industrial policy, and identify recommended actions for Congress and the administration. ■

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 general support from the Department of Defense.

1 Interview with author.