MAY 2021

Mapping the National Security Industrial Base

Policy Shaping Issues

By James Andrew Lewis

Executive Summary

The term "National Security Industrial Base" (NSIB) appeared in the 2018 *National Security Strategy*. The NSIB is the "network of knowledge, capabilities, and people—including academia, National Laboratories, and the private sector—that turns ideas into innovations [and] transforms discoveries into successful commercial products." This report outlines elements of the NSIB and how a commercially driven innovation differs from a defense-centric approach to technology. The U.S. innovation ecosystem is based on a mix of strong research universities, flexible financial systems, a competitive business focus, and risk-taking, entrepreneurial culture that is skilled at commercializing research. Other countries have similar strengths, but not at the same scale.

NSIB Timeline: 1930–2021

The United States has relied on technology to provide a qualitative advantage over opponents since the 1940s. Technological superiority was produced by a superb scientific establishment, long-term federal support for research, and close links between the research and industrial communities. Both support and linkages atrophied in the last few decades. This began in the 1990s and lasted until 2015. In the past, the United States stopped spending when it believed there was no longer any threat to its security. For this, and other reasons, innovation in the United States is now in the private sector, oriented toward commercial markets. The United States realizes it has a problem connecting national security to innovation. Since 2015, the situation has begun to improve, but efforts at change remain underfunded.

Elements of the NSIB

Broadly speaking, the NSIB has three categories of participants: researchers, investors, and entrepreneurs, supported by "soft infrastructure (described in Appendix B). This also includes large companies, which

increasingly see technology as crucial to their success. Innovation is largely independent of the defense industrial base. A clear example of this is that the top five private research and development (R&D) spenders outspent the top five defense prime contractors on R&D by almost ten-to-one in 2018. The defense acquisitions process was designed to manage complex, expensive weapons programs, but most emerging technologies will be developed in the private sector for commercial markets.

A Different Culture and Incentives Undercut National Security Innovation

Mapping national security needs to the innovation base is difficult because commercial incentives and national security needs usually do not line up. The cultures of the NSIB and the conventional defense acquisitions base are different, the key difference being attitudes toward risk. Taking the chance of becoming a "unicorn"—a startup valued at a billion dollars or more—outweighs the certainty of a DOD contract. Contracting can take years, and while there are efforts to streamline the acquisitions process, this system still works best for large, multibillion-dollar programs.

China's NSIB Compared to the United States

The obvious point of comparison is with China. Except in a few key areas, China's innovation system remains weaker than the United States' innovation system. China uses a hybrid state/market model. It still benefits from its trade relations. China's goals are to ensure that its economic development and modernization continues, to end reliance on foreign technologies, and to build a technology base sufficient to produce high-tech weaponry and commercial products that, when combined with subsidies, can displace foreign competitors.

"Military-Civil Fusion" moves China's economy closer to a wartime footing with deep integration of the civilian and defense technological ecosystems, similar to the approach used by the Soviets in the Cold War. The tension in Chinese policy is between central planning and market-driven innovation. The Communist Party's desire for control distorts China's inherent entrepreneurial strength. Privately, Chinese researchers express concern that a tightening political system will slow Chinese innovation, which had increased in a period of relative political openness.

Building on Strength

A dynamic private sector innovation ecosystem is focused on commercial markets, but with the right authorities, funding, and mechanisms, the national security community can take advantage of this. The NSIB could benefit from greater institutional flexibility to partner with American innovators and entrepreneurs, and establish new partnerships with allies. These, along with increased funding for the NSIB, would provide an advantage over China.

Mapping the National Security Industrial Base: Policy Shaping Issues

This is the second in a series of reports looking at how to align the sources of innovation with national security in what has been called NSIB. The term "National Security Industrial Base" appeared in the 2018 *National Security Strategy* and was, according to the authors, a deliberate attempt to move away from the narrower focus implied by "Defense Industrial Base." The strategy **defined the NSIB** as the "network of knowledge, capabilities, and people—including academia, National Laboratories, and the private sector—that turns ideas into innovations [and] transforms discoveries into successful commercial products."

The concept of the NSIB moves the idea of national security beyond military capabilities and defense industries to encompass a broader economic and technological focus that better fits the nature of today's competition with China. This report outlines elements of the NSIB and reviews the issues raised by the difference between a commercially driven innovation system and previous, defense-centric approaches to technology development.

A dynamic private sector innovation ecosystem is focused on commercial markets, but with the right authorities, funding, and mechanisms, the national security community can take advantage of this. This alignment will require some effort because the existing culture for national security technology acquisition is not well suited to innovation. Changing culture is not easy, and some, such as Max Planck or Thomas Kuhn, argue that it is impossible.

Innovation can mean many things. For this series of reports, innovation means the **development and application of technology**. This includes artificial intelligence (AI), quantum computing, biotechnology, cloud computing, microprocessor technologies, data analytics, robots, sensors, and software. Many of these have valuable military applications, but—and in this sense, NSIB is a misnomer—they will be created in the private sector for commercial markets, in what this report calls the national innovation ecosystem. The private sector will outspend the Department of Defense (DOD) in key technology areas and is already the driver of innovation. The task for policy is to identify how to engage the energies of commercial innovation toward national security tasks.

The U.S. national innovation ecosystem derives its immense strength from its mix of strong research universities, flexible financial systems, a competitive business focus on technology, and a fast-moving, risk-taking, entrepreneurial culture. Other countries also have these strengths, but not at the same scale or scope. While there may be dramatic and rhetorical benefits from exaggerating the United States' decline, policymakers should not lose sight of this strength.

America's vibrant innovation system has structural weaknesses, such as the failure to invest in fundamental research, but these are being remedied. It is not that the United States is lagging but that it needs to move faster and better connect commercial innovation to national security. The defense acquisitions process was designed to manage the complex, expensive weapons programs of the twentieth century. It is perhaps the best in the world at this task, but it is reluctant to take the risks associated with innovation. This "cultural" mismatch is one of the principal impediments to national security innovation.

NSIB Timeline: 1930–2021

The United States has relied on technology to provide a qualitative advantage over opponents since the 1940s (see Appendix A for a detailed timeline). Fewer, better weapons could defeat an opponent with a larger military force, as with the Red Army during the Cold War or the Iraqi army in Desert Storm. The United States' qualitative advantage came from the technological superiority produced by

a superb scientific establishment, consistent, long-term federal support for research, and close links between the research and industrial communities. However, both support and linkages atrophied in the last few decades.

While the foundation for the NSIB was laid almost 80 years ago, this timeline shows a decline that began in the 1990s and, with a few exceptions, lasted until 2015. In essence, there was 50 years of investment in national security innovation followed by 25 years of indifference. The United States lost a quarter-century in maintaining its technological advantage. The chief problems in this period, after the lack of focus on strategic competitors, were underfunding and a risk-averse culture often antithetical to innovation. Recovering from this is one of the main challenges for national security, and the last six years have seen the start of many initiatives to accomplish this.

In essence, there was 50 years of investment in national security innovation followed by 25 years of indifference. The United States lost a quarter-century in maintaining its technological advantage.

Since 2015, efforts to "short circuit" a risk-averse culture by creating new institutions have begun to change the situation, but these efforts remain underfunded. DOD, with the exception of the Defense Advanced Research Projects Agency (DARPA), has been slow to take big, riskier bets on innovation. For example, DOD spent $64.5 billion on all **R&D in FY 2020**, but only $29 million for the Defense Innovation Unit (DIU). The budget for AFWERX is similarly small. While this will increase in future budgets, a good comparison is with DARPA's 2020 budget of $3.5 billion. While these program budgets are set to be expanded in coming years, and both organizations will leverage their funding and investments, the majority of R&D spending for national security is still in conventional channels.

The timeline leads to three conclusions: (1) in the past, the United States slowed or stopped federal spending when it believed there was no threat to its security. That's clearly changed, but only after two decades of cuts; (2) the innovation ecosystem in the United States is in the private sector, oriented toward commercial markets; and (3) the United States realized 20 years ago that it had a problem connecting national security to the innovation ecosystem and began a sustained effort to change this in 2015. There has been some progress, but more needs to be done.

Elements of the NSIB

Broadly speaking, the NSIB has three categories of participants: researchers, investors, and entrepreneurs. These include large companies, which increasingly see technology as crucial to success. A rough breakdown for the United States shows:

- There are 945 research universities in the United States, of which 219 have high levels of research activity (according to one **widely accepted ranking**). Another **prominent ranking** identifies 5 of the top 10 research universities as American (and no Chinese universities). Federal support provides about 55 percent of the funding for **academic research**.
- University research is **accompanied by** the work of the 17 National Labs operated by the Department of Energy, 42 Federal Funded Research and Development Centers (FFRDCs) sponsored by 12 different agencies, and military service-affiliated research labs, such as AFRL and NRL.

- There are roughly **1,000 venture capital** (VC) firms (still clustered in California, Massachusetts, and New York, although VCs are appearing in many **states with strong university systems**). These VCs made over 6,000 deals in 2020 and have more than **$156 billion invested** in roughly 11,000 companies.
- Only a few of the big corporate labs, such as **IBM and Bell Labs**, that were leaders in the late twentieth century fundamental research and general-purpose technology still exist, but there has been a resurgence of research at major tech corporations doing AI and quantum-related work.
- Corporations use VC investment to create or acquire innovations. **One survey found** 927 corporations with VC arms. Three-quarters of **Fortune 100 companies** have made VC investments, and slightly more than half have their own venture investment arms. Many corporations have turned to outsourcing or collaborative alternatives to traditional R&D to create customer-focused innovation.
- The U.S. STEM workforce is strong, but could be stronger, and there are persistent shortages in some tech-related workforce areas. The United States has an innate advantage in that its universities remain the **most attractive global destination** for graduate education. One strength is that these universities and (until recently) the American lifestyle draw a highly talented immigrant workforce.
- The 2017 ***National Security Strategy*** notes that "a healthy defense industrial base is a critical element of U.S. power and the National Security Innovation Base." Defense contractors also contribute to the NSIB. Well-known examples of large contractors include firms such as Lockheed's Skunk Works, but small research groups and mid-sized defense firms are also part of the NSIB. The Defense Industrial Base brings immense engineering and technology talent but is not central to the national innovation system.
- **Five high-tech industry sectors** spend heavily on R&D and translate that into products. These are (1) aerospace, (2) pharmaceuticals and biotech, (3) computers, (4) scientific instruments, and (5) semiconductors and communications equipment. These sectors, in combination with universities and start-ups, are the core of what we can call the "national innovation ecosystem."
- An innovation ecosystem depends on intangible elements, or "soft infrastructure"—the culture, educational system, financial sector, and firms offering the business and legal skills needed for success (discussed further in Appendix B). A key part of soft infrastructure is the nexus of business laws and regulations, intellectual property protections, effective courts, and capital markets. Soft infrastructure is as important as "hard" infrastructure (e.g., networks) and spending on research. U.S. soft infrastructure has been one of the strengths of its innovation ecosystem and gives the United States an advantage over competitors.
- This description highlights that the NSIB is now largely independent of DOD and the defense industrial base. **A clear example of this** is that the top five private R&D spenders outspent the top five defense prime contractors on R&D by almost ten-to-one in 2018. Another example is that federal AI spending will increase from **$3 billion to $6 billion** in 2021, while spending by the top five private companies **amounted to $80.5 billion** in 2018. The private sector now drives U.S. innovation. Finding ways to access, guide, and harvest commercial innovation to support national security is a central problem.

Culture and Incentives Work against Innovation for National Security

Mapping national security needs to the innovation base is difficult because commercial incentives and national security needs do not always line up. DOD may not always even be aware of what is available on the market. This is where expanding the entrepreneurial approach seen with DIU, AFWERX, and others

would be useful to be able to identify, invest in, and "harvest" commercial technology. In many instances, DOD is better served in gaining access to innovation if it identifies or modifies commercial technologies for national security purposes rather than pursuing "custom-made" technologies. Commercial space programs are an example. Every DIU prototype dollar generates $15 of VC and private equity investment.

The cultures of the NSIB and the conventional defense acquisitions base are different, the key differences being attitudes toward the acceptance of risk and a focus on commercial markets. In this entrepreneurial culture, taking the chance of becoming a "unicorn"—a startup valued at a billion dollars or more (there are more than **600 unicorns across the world**, mostly in the United States and China)—outweighs the certainty and complexity of a DOD contract.

Tech entrepreneurs often prefer to pursue a big win even if it is risky. This highlights how traditional DOD acquisition contracting does not always fit with the innovation ecosystem. DOD identifies a need, solicits proposals, selects one (often subject to legal challenges by the losing bidders), develops detailed requirements that can run into the thousands of pages, establishes a DOD program office to oversee the project, attempts to see that timelines are met, makes the many changes to requirements that are usually required. The process can take years. While there are efforts to streamline the acquisitions process, this system still works best for large, multibillion-dollar programs.

Compare this to how a company or VC firm identifies investment or acquisitions opportunities. They identify a future market opportunity and then look for technologies or proposed technologies that can meet that market need. They do not develop detailed requirements, though depending on the maturity of the innovating company, they may provide managerial advice. Expectations are different. Out of every ten startups, only one or two will make major profits, and two or there will fail.

There is a contentious discussion about the productivity of the various elements of the NSIB, measured by "innovation" outcomes. Innovation is itself hard to measure. Traditional innovation metrics use "proxy" measures, such as the number of patents or PhDs, but these can be problematic. First, there is an assumption of causality—more patents mean more innovation—but this is not a one-to-one correlation. Second, as some countries, particularly China, have realized that these proxy measures are used to assess technological strength, they "game" the system by increasing the number but not the quality of publications or patents, thus leading to a greater measure of innovation. Nor is spending on R&D necessarily a good indicator of success. A long-running **survey by PWC** found no correlation between dollars spent on innovation and companies' financial performance, suggesting that how money is spent by a company is as important as how much is spent.

The same is not necessarily true for national spending on R&D, but it points to the risks in government investment programs. If the program tries to pick winners too early or if R&D spending is not accompanied by entrepreneurship, there may be inadequate returns. Income is probably a better metric, using revenue for individual companies and national income for countries. These are not precise since other factors affect income levels and trends.

One thing to note is that innovation is a distributed process. There are thousands of actors. A top-down approach where the government tries to direct this system is self-defeating.

One thing to note is that innovation is a distributed process. There are thousands of actors. A top-down approach where the government tries to direct this system is self-defeating. It helps to think of the NSIB as an innovation "market." Markets are a good model for understanding how distributed systems organize. They do this by using incentives and "signals." Movements in these signals (usually prices) tell investors and entrepreneurs where demand for products and services will be and what they should spend on. Coordination results as each actor responds independently to these price signals.

The incentives currently signal that actors should focus on commercial products and services rather than the national security market, and on software rather than hardware. The commercial market for technology dwarfs the "Total Addressable Market" in defense. Demand for software goods and services, a focus for American entrepreneurs, is high and will likely increase as 5G networks create new possibilities. The barriers to entry for would-be entrepreneurs are low for software and higher for hardware. Hardware is where targeted federal spending in areas where commercial and national security interests overlap can change the incentive structure enough to attract innovators and overcome this.

China's NSIB Compared to the United States

A quick review of China's national security innovation system shows that it is, except in a few key areas, weaker than that of the United States. China uses a different model for national security innovation. It has a hybrid state/market innovation base, modeled in part on U.S. practice. China benefitted, and still benefits, from its trade relations with market democracies and uses a mix of investment and market access policies for technology transfer. The tech communities in both countries are still connected. The United States' soft infrastructure and "installed base" for innovation remains stronger than China's, but in this competition, China retains one clear advantage: it has been willing to invest in its science and technology base. China's goals are to ensure that its economic development and modernization continues, to end reliance on foreign technologies, and to build a technology base sufficient to produce high-tech weaponry and commercial products that, when combined with subsidies, can displace foreign competitors.

China's policies are increasing government control, which could hamper innovation, but China's willingness to spend may compensate for this. China has already made significant strides in quantum encryption, AI, autonomy, (especially in autonomous cars; China has designated autos as a "core strategic industry"), and biotech, although Chinese investors still prefer to spend on U.S. biotech companies. Chinese private sector innovation is strong in AI, autonomous vehicles, and other areas. China leads in digital currencies and benefits from its strong manufacturing base. It has a strong "app" economy for fintech and software products that take advantage of mobile devices.

If one compares elements of the United States and Chinese innovation systems such as VCs or research universities, some U.S. advantages become clearer. Chinese sources say there were 14,000 registered VCs in China in 2019, coming at the end of a 10-year boom in venture capital. However, the level of investment and the number of deals declined from 2018 to 2019, driven by uncertainty over regulation, the U.S.-China trade war, and what Chinese investors themselves describe as a **lack of commercially appealing innovation**. This downturn could be cyclical but may also reflect permanent changes because of decoupling and Xi Jinping's economic policies.

Chinese educational policies emphasize building a STEM workforce. While there are concerns about the quality of Chinese STEM graduates, these concerns are declining as STEM education improves, and China, with a population of over 1.4 billion people, has an absolute quantitative advantage. China has many universities, but none are yet at the top for research. **University rankings** place Tsinghua,

the highest-ranked Chinese university, in 15th place, and the next highest, Peking University, comes in at 23rd. Of the top 50 universities in the world, only 4 are Chinese (the absorption of Hong King may boost the number if staff remains). While China claims that in the next 10 years, it will double spending devoted to basic research, the relatively weak research base reduces the benefit of government spending. One exception to this is in biotechnology research, where **three Chinese research centers** are among the world's leaders. Overall, however, China still depends on foreign universities and research for innovation inputs. China's own plans call for making **98 of its universities** world-class institutions by 2050.

Government-affiliated research centers still play a major role in national security innovation in China, and work by the **Australian Strategic Policy Institute** shows a growing number of civilian universities are involved in military research and related espionage.

China's coupling of its innovation base to national security creates strong linkages but may come at a cost to the overall ability to innovate. A "**Military-Civil Fusion**" moves **China's economy** closer to a wartime footing, **with a deep integration** of China's civilian and defense technological ecosystems. In contrast to the United States, in China, national security has become the dog that wags the innovation tail. This is similar to the approach used by the Soviets in the Cold War and the United States in World War II, raising the question of the degree to which America should copy it. But there are two scales on which to measure any answer: the ability to link innovation to the needs of national security and the productivity of the innovation base. The decentralized, market-driven U.S. national innovation base can be more productive, meaning that if the United States can find better ways to harness this for national security problems, it can outperform China.

Policies in China have for some time emphasized domestic, or indigenous, innovation. In 2006, China's State Council issued "Guiding Principles" for scientific and technological development that made improving indigenous innovation the most important aspect of science- and technology-related work, using tax incentives, financial support and technological investment, and government preferences for Chinese technology.

China wants to move from assembling final products from imported components to creating advanced technology in China itself. To that end, they have used massive government investments in infrastructure, education, and research, along with both licit and illicit technology acquisitions and supportive commercial and trade policies, to produce economic growth and build an innovation base. However, Chinese innovation increased in a period of relative political openness. Now that openness is shrinking under Xi Jinping, accompanied by greater state economic direction, it is possible that Chinese innovation will slow or reverse.

China's innovation and technology sector has vulnerabilities. Centrally directed economies can be less efficient, since government policy supplants markets. China is aware of the "Gosplan" risk but is also genetically predisposed to commit it. Easy access to funding removes competitive pressures that produce greater returns. China is not a market economy, but neither is it a Soviet-style command economy, although the central government increasingly directs investment toward strategic goals. The multinational nature of research and innovation complicates any national competition for technological leadership, and an internationally focused United States may have an advantage over a nationally focused China.

The multinational nature of research and innovation complicates any national competition for technological leadership, and an internationally focused United States may have an advantage over a nationally focused China.

The tension in Chinese policy is between central planning and market-driven innovation. The source of this tension is the Chinese Communist Party's (CCP) desire to control the political effects of successful entrepreneurship. If the direction between 1980 and 2010 was toward greater decentralization and privatization, these trends have now been reversed. As a general rule, decentralized, market-oriented innovation systems are more likely to be productive than centrally directed government programs. But this innovative sector was only weakly connected to China's military and faces a procurement breaker at least as burdensome as that faced by tech companies in the United States. Privately, Chinese researchers express concern that a tightening political system will slow China's innovation capabilities.

The United States leads in semiconductors, software, and 5G and 6G, and has a softer lead in AI, quantum, and biotech. China depends on the United States for semiconductor manufacturing equipment and advanced chips (although it is striving to end this). The U.S. national innovation base has inherent advantages over China, but it should not let these advantages blind it to China's strengths.

Building on Strength

Culture is a crucial aspect of innovation and entrepreneurship. While there is some risk of falling into crude stereotypes, a simple division would show the United States as the most risk-tolerant, **Europe as the least**, and **China as somewhere in the middle**. A review of open-source literature shows that U.S. strengths are in entrepreneurship and in an innovation base (the institutions and actors identified in later) that is skilled at commercializing research. China is strong in entrepreneurship (although its expanding domestic political controls may harm this), but its innovation base is still weak. Europe has a strong innovation base but is weaker in tolerance of entrepreneurship and risk.

None of these advantages or disadvantages is necessarily permanent, and the Chinese government even has programs to encourage greater tolerance of commercial risk. China can use its centrally directed investment strategies and incentives to strengthening its innovation base, but its leaders are reluctant to accept the political risk that entrepreneurship could create—the fate of Jack Ma is instructive for Chinese entrepreneurs. This desire for continued political control by the CCP distorts China's inherent entrepreneurial strength.

This also suggests the NSIB could benefit in two ways: greater flexibility to partner with American innovators and entrepreneurs and new partnerships with allies in Europe and Asia. These would provide benefits when compared to China, along with increased funding for nontraditional approaches to acquiring innovation for national security needs. The task is to forge a new relationship between national security and innovation in very different circumstances, the most important changes being the centrality of private actors with different expectations and incentives for innovation and the "multilateralization" of innovation and research.

The United States has always been willing to spend what is needed for defense. Investment in technology is now a requirement for defense in this conflict. Federal investment would provide both economic and military benefits. The United States spent perhaps $6 trillion over the last 18 years in Iraq and Afghanistan. Investing a fraction of this in maintaining technological leadership would have strengthened the United States' ability to compete with China. This was a missed opportunity, even a strategic blunder, but it is not too late to repair it. The next report in this series will look at how to overcome the challenges of linking the national innovation ecosystem to national security and what policy tools exist for the NSIB or need to be developed. ■

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

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

Appendix A: National Security Innovation Timeline, 1930–2015

- **1930s:** The federal contribution to basic research in the 1930s averaged only a third of a percent of GDP and was even less for military procurements.
- **1940s:** Science and technology became a force multiplier in World War II, and the United States developed institutions to link its scientific community to national security problems. The National Defense Research Committee (NDRC) and the Office of Scientific Research Development were established in 1940 to mobilize and organize research for military purposes and to develop new technologies and operational strategies. The **experience was summarized** in Vannevar Bush's study *Science: The Endless Frontier*.
    - The Manhattan Project is the best-known example of the use of science in World War II, but it was accompanied by decisive advances in anti-submarine warfare, encryption, computing, radar, aircraft engines, and rockets. All depended on physics, chemistry, mathematics, and engineering.
- **1950s:** Presidents Truman and Eisenhower made federal support for a strong research community part of national security. The creation in the 1940s and 1950s of the Office of Naval Research, Atomic Energy Commission, National Laboratories, NASA, and National Science Foundation institutionalized this support.
    - The 1957 launch of Sputnik shocked the United States and led to predictions that Soviet superiority in math and science education would give it global leadership within a decade. In response, the United States created the Defense Advanced Research Projects Agency (DARPA) with the mission to ensure military superiority for the United States by nurturing technological innovation. Congress passed the National Defense Education Act (NDEA) to subsidize education in the sciences, mathematics, and foreign languages.
- **1970s:** In the 1970s, when it became apparent that the United States would not be able to match the quantitative advantage of the Soviet bloc in conventional weapons, William Perry, then the undersecretary for acquisitions, committed DOD research efforts to technologies that would overcome the Soviet numerical advantage. His investments in precision guidance, stealth, sensors, and communications created a "revolution in military affairs."
- **1990s:** The 1990 Persian Gulf War showed that the use of then-new technologies, including space-based sensors and better communications, combined with precision munitions gave the United States a surprising advantage (at least to opponents).
    - The CIA created In-Q-Tel in 1999 to identify and invest in companies developing new technologies for national security.
- **2000s:** The Defense Authorization Act legislates a "non-profit Army venture capital corporation," which led to the Army Venture Capital Initiative 2002, originally funded at $25 million and intended to establish better ties to start-ups "that take risks and push innovation."
    - In 2001, the Navy created "**Swampworks**" for innovative technology development but allocated it less than 1 percent of the Navy's science and technology budget.
    - The 2004 National Military Strategy recognized that "disruptive future challenges are those likely to emanate from competitors developing, possessing, and employing breakthrough technological capabilities," an example of an early recognition of the national security innovation

problem, but action was hampered by budget concerns and a refocusing of R&D on the operational challenges from ongoing wars in the Middle East.

- **2010s:** The Defense Technical Information Center created the Rapid Innovation Fund in 2011 to bring innovative technologies into defense acquisitions programs. Perhaps not as rapid as the name would suggest, it was cut in 2020.
    - In 2014, DOD created the Defense Innovation Initiative, spawning a host of efforts to increase access to new technologies at DOD.
    - Worried that DOD had lost access to commercial innovation, then-secretary of defense Ash Carter created DIUx (Defense Innovation Unit Experimental) in 2015.
    - Carter also established the Defense Innovation Board (originally called the Defense Innovation Advisory Board) in 2016 to bring "Silicon Valley innovation" to the U.S. military. One of the board's most significant contributions included the recommendations that led to the creation of the Joint Artificial Intelligence Center.
    - The new emphasis led to a number of smaller DOD "start-ups" and tech accelerators, including AFWERX (created in 2017), SOFWERX, and the (renamed) National Security Innovation Network, created to connect innovators and entrepreneurs.
    - The "x" is removed from DIUx in 2017, and it is re-designated as the Defense Innovation Unit to indicate both the success of DIUx and the DOD intention to make it permanent.

Appendix B: Soft Infrastructure

An innovation ecosystem depends on intangible components, or "soft infrastructure"—the culture, educational system, investors, and firms offering the business and legal skills needed for success. A key part of soft infrastructure is the nexus of business laws and regulations, intellectual property protections, effective courts, and capital markets. Soft infrastructure is as important as "hard" infrastructure (e.g., networks) and spending on research. Soft infrastructure minimizes the risk for entrepreneurs as they turn research into innovations.

U.S. soft infrastructure has been one of the strengths of its innovation ecosystem and gives the United States an advantage over competitors. But mapping soft infrastructure, which was created around commercial requirements, to the federal rules and regulations that govern government acquisitions could be an obstacle to linking national security access to innovative technologies. For a quick overview of soft infrastructure for mapping the NSIB, one should look at the core elements.

- **Flexible Financial Systems:** A good starting point for a discussion of financial flexibility is to recall when Henry Ford's banker said, "the horse is here to stay, but the automobile is only a novelty—a fad." Conventional banks are risk averse. Since Ford, banks have developed a range of financial and investment arms, but the innovation ecosystem is supported by a division of labor among investors and financial institutions that provides support in the initial phases of a technology's development and commercialization until it is ready to be supported by conventional financing.

  VC firms and start-ups are a core part of the commercial innovation system, with its intensely commercial focus, but they are not the only source of innovation. The number of VCs fluctuates with the economy, and the U.S. share of VC firms has shrunk from 80 percent to 50 percent in the last 15 years. The larger **VC ecosystem** includes investors who specialize in different stages of start-up development, such as angel investors and now also "crowdfunding," where many investors provide relatively small amounts, usually in exchange for some equity in the firm, but this kind of alternative finance provides less than 2 percent of annual investments. In an idealized scenario, angel investments lead to VC firms, which then guide the start-up private equity investments to an initial public offering (IPO).

  They are not the only path to innovation, of course, but they are perhaps the most dynamic element. Reconnecting national security and innovation means investing in small, entrepreneurial firms that are outside of the traditional defense industrial base. VCs are not a perfect model, since their goals are different—DOD is hunting for technologies, not deals—but VCs can be a useful entry point into the innovation ecosystem.

  Tangled connections are the norm in venture capital, 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 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.

- **Human Capital: Human capital** is the stock of individuals with the education and experience needed for innovation. A strong human capital foundation is crucial for innovation. Investment in human capital helps national security in other ways. The United States' opponents exploit the discontent over inequalities in opportunity and income. Expanding the science and technology workforce helps national security.

  While not a perfect indicator for innovation skills, one measure for human capital is that the United States has the highest share of knowledge- and technology-intensive (KTI) industries as a proportion of gross domestic product (GDP) of any large economy. It also has had the **highest concentration of KTI industries** among major economies, which generate 40 percent of U.S. GDP, compared to 30 percent for the European Union and Japan and 20 percent for China. China's economic growth means, according to the National Science Foundation, that it is now comparable to or exceeds that of the United States in some KTI industries.

  Support for basic research is essential for a strong NSIB. Basic research expands the pool of knowledge used to find solutions to national security problems and supports the research and engineering that produce both new technologies and a technological workforce. The United States misjudged the new strategic environment and underinvested in defense innovation and research in key areas—basic research in physics, mathematics, computer sciences, and engineering. These disciplines provide the basis for military advantage, create the workforce for sensitive projects, enable other sciences, and are a source of economic growth. Measured as a share of GDP, their funding has decreased steadily for decades, but fortunately, this trend is now being reversed.

  The United States revolutionized its military when, with its British allies, it began to apply science to military problems in World War II. This required the recruitment of scientific talent to work on technological solutions to military problems. The United States benefitted from the outflow of leading scientists from Europe in the 1930s. This influx of scientific talent became one of the foundations of U.S. technological leadership. In addition to accessing the foreign talent pool, the technology workforce was given an additional and long-lasting boost by the U.S. reaction to *Sputnik*, which involved a significant increase in funding for research and for STEM education.

  This *Sputnik* boost ended in the 1990s and was not replaced. While the United States remains preeminent in scientific education and research (often at institutions founded by European scientific émigrés), it has reduced the number of its own citizens being educated and does not aggressively seek to retain enough of the scientific talent it graduates. In effect, the United States has reversed the workforce policies that gave it technological advantage for 50 years.

- **A Risk-Tolerant Culture:** Culture is important when considering a willingness to take risk, accept failure, and disrupt (an overused word) the business status quo. A country can have a strong research base and powerful companies with a skilled workforce and still not be particularly innovative. To use France as an example, it has a skilled workforce and a strong research base, but until recently it has had difficulty commercializing this research. Attitudes toward failure are an important element of success in innovation.

- **Intellectual Property (IP) Protections and Tech Transfer:** The laws protecting intellectual property are important in two ways. First, by ensuring a financial return on invention, they incentivize inventors and researchers by providing them a monopoly on patentable inventions. Because a

patent is published when it is granted in the United States, this allows other inventors to identify related areas of valuable research and build on discovery. Since the monopoly provided is limited in duration, it means that other inventors can copy and improve the patented innovation after a period of time.

Tech transfer, in this case, does not refer to transfer among countries, but ownership of the products of academic research. While there can be frictions in the process, the United States allows researchers and universities to develop commercial products from research it has funded. This creates a powerful incentive for innovation.