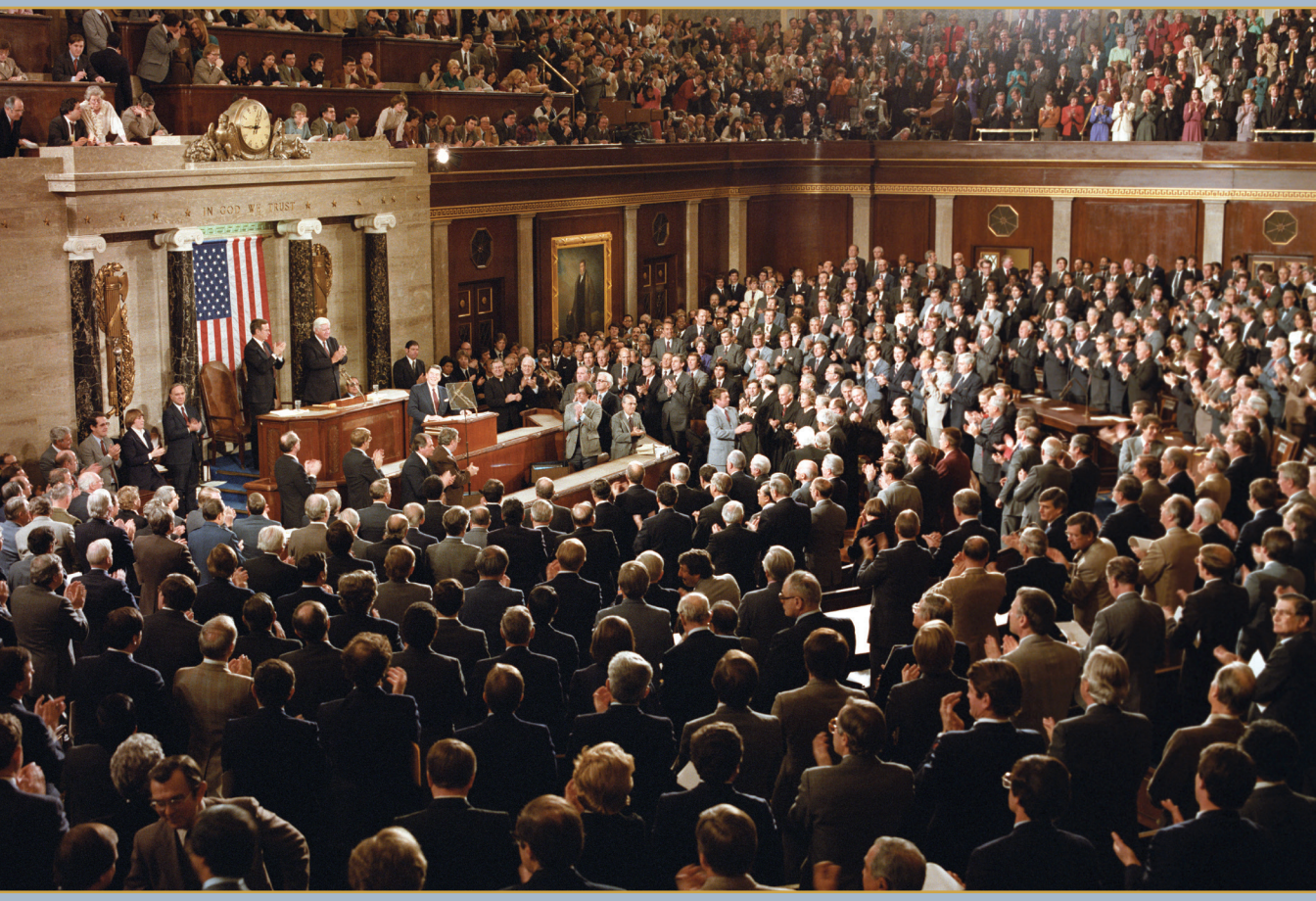
RONALD REAGAN INSTITUTE

The Contest for Innovation:

Strengthening America's National Security Innovation Base in an Era of Strategic Competition

Report of the Task Force on 21st-Century National Security Technology and Workforce



"As surely as America's pioneer spirit made us the industrial giant of the 20th century, the same pioneer spirit today is opening up on another vast front of opportunities – the frontier of high technology."

- President Ronald Reagan

RONALD REAGAN
INSTITUTE

The Ronald Reagan Institute, the Washington, DC, office of the Ronald Reagan Presidential Foundation and Institute, promotes our 40th President's ideals, vision, and leadership example through substantive, issue-driven forums, academic and young professional programming, and scholarly work.

Table of Contents

Task Force Co-Chairs

The Honorable Jim Talent
Senior Fellow, Bipartisan Policy Center
Former U.S. Senator (R-MO)

The Honorable Robert O. Work
Distinguished Senior Fellow, Center for a New American Security
Former Deputy Secretary of Defense

Task Force Members

Ms. Lisa Atherton
President and CEO, Textron Systems

Congressman Jim Banks (R-IN)
Lieutenant, U.S. Navy Reserve

Mr. Christian Brose
Head of Strategy, Anduril Industries
Former Staff Director, U.S. Senate Committee on Armed Services

Ambassador Eric S. Edelman
Counselor, Center for Strategic and Budgetary Assessments
Former Under Secretary of Defense for Policy

Congressman Mike Gallagher (R-WI)
Former Captain, U.S. Marine Corps

Congressman Andy Kim (D-NJ)
Former National Security Official

Congresswoman Stephanie Murphy (D-FL)
Former National Security Specialist, Department of Defense

Mr. Donald J. Rosenberg
Executive Vice President, General Counsel and Corporate Secretary, Qualcomm Incorporated

Dr. Nadia Schadlow
Senior Fellow, Hudson Institute
Former Deputy National Security Advisor for Strategy

Mr. Raj Shah
Co-Founder and Chief Executive Officer, Arceo.ai
Former Head, Defense Innovation Unit

Mr. Matthew Waxman
Professor, Columbia Law School
Former Principal Deputy Director of Policy Planning, Department of State

Ronald Reagan Institute Staff

Roger Zakheim
Director, Ronald Reagan Institute

Rachel Hoff
Policy Director, Ronald Reagan Institute

Keeghan Sweeney
Special Assistant to the Director, Ronald Reagan Institute

Task Force Senior Advisors

Robert Atkinson
Founder & President,
Information Technology and Innovation Foundation

Samantha Clark
Former Deputy Staff Director and General Counsel,
Senate Armed Services Committee

Jeffrey Dressler
Former National Security Advisor,
Office of Speaker of the House Paul Ryan

Ben FitzGerald
Adjunct Senior Fellow,
Center for a New American Security

Alex Gallo
Executive Director, The Common Mission Project

Bill Greenwalt
Senior Fellow, Atlantic Council

Col. Wesley Hallman, USAF (Ret)
Senior Vice President,
National Defense Industrial Association

Gayle Tzemach Lemmon
Partner & Chief Marketing Officer, Shield AI

John Luddy
Vice President for National Security Policy,
Aerospace Industries Association

Zachary Mears
Former Chief of Staff, Office
of the Deputy Secretary of Defense

Larry Rubin
Associate Professor, Sam Nunn School of International Affairs,
Georgia Institute of Technology

Trae Stephens
Partner, Founders Fund

Nate Walton
Principal, Sachem Strategies

Keith Webster
President, Defense and Aerospace Export Council,
U.S. Chamber of Commerce

Ali Wyne
Policy Analyst, RAND Corporation

Task Force Briefers

Michael Brown
Director, Defense Innovation Unit

Gabrielle Burrell
Minister Counsellor Defense Policy,
Embassy of Australia in Washington, DC

Eric Chewning
Chief of Staff, Department of Defense

James Cross
Vice President, Franklin Equity Group

William Evanina
Director, National Counterintelligence
and Security Center

Edward Ferguson
Minister Counsellor Defense,
Embassy of the United Kingdom in Washington, DC

Elsa Kania
Adjunct Senior Fellow, Center for
a New American Security

Frank Kendall III
Former Under Secretary of Defense for Acquisition,
Technology and Logistics

Ellen Lord
Undersecretary of Defense for Acquisition
and Sustainment

Chris Lynch
Former Founding Director, Digital Defense Service

Tom Mahnken
President and CEO, Center for Strategic
and Budgetary Assessments

Theresa Mayer
Executive Vice President, Purdue University

Milo Medin
Vice President, Google

The United States has entered an era of long-term competition with revisionist powers. A key aspect of this competition will revolve around a contest for technological superiority waged between the national innovation bases of the respective competitors. The outcome of this competition will determine not just American national security but also how the nations of the world interact—and whether a free and open political and economic system will remain the foundation of those interactions.

After a long post-Cold War focus on rogue regional powers and nearly two decades of continuous warfare in the Middle East and a focus on rogue regional powers, the United States now faces a new defining national security challenge: a long-term strategic competition with a resurgent Russia and a rising China.

Russia seeks to reestablish itself as a global power. While Russia is able to compete with the United States militarily in certain domains, its economic outlook and long-term demographic prospects are grim. Accordingly, it is unlikely to develop and nurture a true national innovation ecosystem. Given these disadvantages, Russia is limited to acting as a geostrategic spoiler seeking to undermine and weaken the United States, its alliances, and its global interests.

China, on the other hand, is already challenging the United States economically, militarily, and politically. China's economy has surpassed that of the United States in terms of purchasing power parity and could, under some scenarios, pass the U.S. GDP in absolute terms in the mid- to late 2020s. Under the leadership of the Chinese Communist Party, China defines its vital national interests in ways that are irreconcilable with both the interests of the United States and the values of self-determination and individual freedom to which we and our allies are committed. China's global expansion, from both a trade and military perspective, is challenging the United States in virtually every region of the world.

In pursuit of its goal of reshaping the world order, China aims to supplant the United States as the world's leading technological power by 2030. China has articulated a distinct strategy of state-driven innovation, defined by its concept of "military–civil fusion," to lead the world in cutting-edge technologies that might allow it to leapfrog the United States both economically and militarily.

That strategy presents a two-fold challenge for the United States. Economically, the challenge is to sustain American prosperity and access to markets on equal terms with other nations against China's ambition to control the economic sectors that will determine national primacy in the decades ahead.

Militarily, the fundamental mission of the U.S. government (USG) is to deter a great-power war and, if deterrence fails, to prevent escalation of the conflict and end the war on terms favorable to the United States and its allies. An important key to this mission is achieving and maintaining military–technical superiority. However, over the last several decades, China—and, to a lesser extent, Russia—has invested heavily in advanced military capabilities specifically aimed at overcoming the technological lead of America's armed forces.

As a result, the conventional overmatch that the United States has relied upon to undergird its deterrence posture since the end of the Cold War is eroding. The balance of power in East Asia has already shifted substantially in China's direction. If this trend continues, effective deterrence in that region will likely fail, leaving the United States to face the unattractive alternatives of accepting aggression against its interests or its allies or triggering armed conflict with the People's Liberation Army (PLA), with all the attendant risks of escalation.

The National Security Strategy recognized the importance of technological innovation to every domain of the competition with China. Consistent with that, a key theme of the 2018 National Defense Strategy is that the U.S. military must move rapidly to arrest further erosion of its technical advantage and then restore and maintain a comfortable conventional overmatch.

Unfortunately, the technological development relevant to national security is no longer exclusively or even primarily in the control of the Department of Defense (DOD) and its prime contractors.

In the past, cutting-edge technology was usually developed by the government sector for military use and then migrated into the civilian sector. Today, the direction of innovation has reversed. Many of the technologies most important to national security are being developed and produced for civilian purposes by civilian actors who have no history with or connection to the national security community. China is aware of this new reality. Its policy of military–civil fusion seeks to better exploit dual-use technologies originating from the commercial sector. To avoid a crippling competitive disadvantage, the United States must adopt means to accomplish the same end.

Accordingly, the most important question this Task Force grappled with was the following: How do we transform, organize, sustain, and leverage our national security technology and innovation community to prevail in a long-term competition against an authoritarian regime that has centralized, long-range national plans to dominate the critical dual-use technologies central to future economic and military competitiveness?

Our findings and recommendations offer some answers to the questions *who, what, when*, and *how*. As we address those points, however, we pause to explain *why*. Why did the Task Force take on this project, and why should the United States consider the policy options outlined in this report?

To answer those questions, we adopted an approach that several of us learned and applied as military officers, diplomats, and planners: orient on the competitor. What would the world look like if China, and not the United States, was allowed to define the ways that countries and people interact, both with each other and with new technology?

Imagine that the Chinese Communist Party, through its control of China's economy, is allowed to set the global ground rules for the next generation of technology. Imagine phones, tablets, and computers that do not function unless they conform to Chinese standards and censorship requirements or that contain materials that can transmit to Beijing a record of everything that is written, stored, and shared online. Imagine further that authoritarian leaders, armed with class-leading technologies like artificial intelligence, facial recognition, and quantum computing, turn that awesome computing power against people and their data. Imagine finally how autocrats might be able to coerce citizens by leveraging this power.

A real-life example is before us today. Witness the treatment of the million men, women, and children in Xinjiang that Chinese officials identified and targeted with the help of facial recognition technology and data-scraping tools. Innocent people have been rounded up into concentration camps for "reeducation" in Communist Party dogma. That is Beijing's policy toward its own citizens. How much restraint would China show toward those it deems "outsiders"?

We offer this narrative to explain why the subject of this report is so important. Competition with China need not lead to warfare or even to a policy of containment like the framework that characterized the U.S.–Soviet relationship during the Cold War. Nevertheless, it is a competition, and the side that innovates more effectively over time is likely to win. The result will determine whether nations relate to each other freely, equally, and peacefully, with a recognition of the human rights of their citizens, or if they devolve into a system that legitimizes authoritarianism and rewards power and coercion.

Surveillance cameras mounted on a post at Tiananmen Square in Beijing, China.

Defining the National Security Innovation Base

The United States is experiencing a technological tsunami. Major technological innovations are combining to disrupt the future of the global economy, warfare, and competition by means short of war. Many of these innovations and the technologies that support them will have direct political, military, and economic impacts on the United States and other free and open societies. And these innovations are dual-use technologies being developed in the commercial sector rather than the traditional defense industrial base. In addition, important innovation is occurring outside of the United States, and even domestic innovation often occurs with foreign investment and supply chains or is subject to foreign influence.

As a result, these technologies are largely accessible to nation-state competitors as well as non-state actors. It is vital for the U.S. government to leverage and protect those technologies. We must also understand and hedge against the extent to which they cannot be protected.

It is also vital that the United States maintain or where necessary regain its advantage across these technologies. Doing so will require common purpose and coordinated effort among a large group of stakeholders, from the traditional defense and national security community to private-sector companies and academia—what the National Security and National Defense Strategies referred to as the National Security Innovation Base (NSIB).[1]

NSIB Definition

The NSIB comprises the ecosystem of capital, research, knowledge, capabilities, policies, incentives, and people that turns ideas into innovations and transforms discoveries into useful technology and products to protect our national security.

The NSIB includes a diverse set of segments, including national security agencies and organizations, the National Laboratories, Federally Funded Research and Development Centers (FFRDCs) and University-Affiliated Research Centers (UARCs), the higher academy, traditional defense "primes," the commercial sector, venture capital, and the innovative systems of American allies and partners.

These segments are often cooperative, but they are loosely federated and largely uncoordinated by the government.

America's ability to prevail in a long-term strategic competition with China depends on a strong and growing NSIB. That in turn depends on more effectively aligning government policy and resources and public–private partnerships to strengthen U.S. national security and its strategic position with respect to China.

The U.S. NSIB has formidable strengths.

- Most segments of the NSIB are world leaders in their respective domains.
- The U.S. economy remains the wealthiest and most dynamic in the world.
- There is strong bipartisan support for national efforts to outpace China, enhancing the likelihood of government prioritization of the problem.
- The private sector is often effective at achieving breakthrough technologies. The free flow of capital and talent has historically made the United States the premier place to launch new companies.
- Moreover, there is precedent for successful cooperation among various segments of the NSIB ecosystem. The space program continues to be a prominent example.

However, the NSIB also has considerable weaknesses.

- The federal government has yet to prioritize effectively the most important efforts or to align political capital and resources against those priorities.
- While the traditional prime contractors are experts in applying innovation to defense systems, they are not necessarily the best agents of innovation themselves.
- The private sector is not yet collectively conscious of the importance and nature of the U.S.–China competition.
- There is insufficient coordination among NSIB segments toward common goals.
- Private-sector research and development (R&D), while substantial in absolute terms, is heavily weighted to development and commercialization and is an inadequate replacement for basic and applied research historically funded by the U.S. government.
- The private sector is competing and often losing against the resources of the Chinese state.
- NSIB security and counterintelligence efforts remain inadequate.
- NSIB stakeholders must work through regulations and processes that prioritize goals other than speed and innovation.
- The NSIB human capital base is aging and struggling to recruit technical talent in key areas.

Measuring and Assessing the Competition

Without question, China is the chief pacing technological competitor to the United States. It explicitly seeks to supplant the United States as the world's top innovation power. Toward this end, China has embarked on an aggressive plan of military–civil fusion focused on critical and emerging technologies. This plan has the potential to disrupt global stability and ultimately undermine the security and prosperity of the United States and its allies.

China's military–civil fusion concept draws from the U.S. model of the Defense Advanced Research Projects Agency (DARPA) and federally funded laboratories but represents an attempt to leverage all aspects of the civilian economy on behalf of national defense.[2] It is characterized by comprehensive government direction, support, and funding for "national champion" companies and mandated coordination among the academic, private sector, and military spheres. This military–civil fusion concept appears especially well-suited to exploit the dual-use technologies central to the 21st-century military–technical competition.[3] Thus, the U.S. NSIB must compete against a Chinese innovation base that uses top-down, long-term planning to exploit innovation wherever it might occur—be it in the business, academic, or government sectors.

Under its authoritarian leaders, the Chinese innovation system leverages forced tech transfer, industrial espionage, and outright theft to access foreign breakthrough technologies and strengthen its own innovation base. China can therefore focus on innovating incrementally and commercializing quickly.[4] Additionally, China's exploitation and theft of U.S. intellectual property (IP) continue to rob the United States of substantial economic value and technological leadership in numerous fields. The United States is losing between $400 billion to $600 billion per year in IP theft as a matter of provable losses—and that figure does not account for second-order losses, such as jobs and infrastructure.[5] Chinese theft has robbed certain companies of game-changing innovations, taking them out of the marketplace or destroying them entirely, with Chinese companies adopting and selling those innovations.[6]

China uses American patents without paying licensing fees and exploits outdated U.S. patent laws to appropriate and scale American innovations before they are even subject to review by our own government. Further, China is leveraging its growing trade power and attractive consumer market

to force legal tech transfer as a condition of doing business with China.[7] Joint ventures with highly unfavorable tech-transfer provisions are being forced upon companies and countries seeking to trade with or sell to China's fast-growing markets, both consumer and enterprise. Finally, China influences other nations both large and small by conditioning trade on the purchase and use of Chinese technology. This type of coercive behavior has spurred a debate over whether engagement with China costs more than separation or "de-coupling" from China.

China aims to leapfrog the United States by adopting new, transitional technologies, in some cases produced cheaply and at scale, while the United States remains attached to legacy systems that will be of value in the near future but will not be sufficient to support U.S. strategy in the medium- or long-term.[8] China seeks to equal or surpass the United States in strategic, frontier technology—such as AI, 5G, biotech, advanced autonomous systems, and quantum computing—while neutralizing the U.S. capabilities that pose the greatest threat to its regional supremacy.[9] China has recognized that global adoption of rules and standards often dictates the pace of innovation, so it strives to establish its technology beyond its borders. This raises issues with Chinese control of that technology and threatens U.S. leadership in R&D investment and innovation.

American universities are key links in developing new technologies, and China deliberately targets them by exploiting the vulnerabilities inherent in the open educational and research environment.[10] Beijing has a focused and resourced effort to do so through a sustained strategy of technology transfer at universities. This campaign includes both Chinese nationals (witting and coerced) and non-Chinese nationals.[11] The USG, academia, and industry must work closely together to increase transparency and accountability for defense and dual-use research at universities and understand Chinese government efforts to benefit from it.

For all its strengths, the Chinese system of innovation also has its own key weaknesses. China is beginning its drive for military–civil fusion from a position of disadvantage compared with the United States, with potential seams between its industry, academia, and the defense establishment. In the past, China's state-owned enterprises were almost entirely responsible for military research and procurement. Now the regime is trying to incorporate other sectors of the economy with little past experience in defense pursuits. China faces other challenges across several areas of technology—including semiconductor manufacturing, AI, and 5G—due to lack of human capital, supply-chain threats, and the difficulties in operationalizing its concept of military–civil fusion.

In addition, notwithstanding certain pockets of success with innovations such as facial recognition technology, China has not yet demonstrated the ability to innovate organically from inception to implementation as comprehensively or consistently as the United States. However, the United States can ill afford to assume this will always be the case.

Ultimately, the Chinese system may have the seeds for its own downfall: corruption remains a major problem; the private sector is becoming increasingly politicized; and the culture of state-owned enterprises, which dominate its defense sector, is vastly different from the culture of its more entrepreneurial companies.

The U.S. NSIB retains fundamental advantages if U.S. policymakers, industry leaders, investors, and technologists can better harness and exploit them.

The U.S. NSIB retains fundamental advantages if U.S. policymakers, industry leaders, investors, and technologists can better harness and exploit them. While it will be important to better protect the NSIB from Chinese theft and exploitation, a defensive posture alone will not be sufficient to prevail in the contest for innovation. The United States must adopt policies that better coordinate the various elements of the NSIB ecosystem, encourage rapid development and adoption of the most important technologies, and ensure that national security technology is developed even where it does not have a profitable commercial application. All of this must be done without inhibiting the freedom and dynamism that are the greatest strengths of the U.S. NSIB.

Despite the weaknesses in China's innovation system, the USG should assume China's determined military–civil fusion efforts will pay substantial dividends over time. Whether or not these dividends will allow the Chinese to pass the United States as the world's technological leader will depend less on Chinese actions and more on those of the United States.

Whether or not these dividends will allow the Chinese to pass the United States as the world's technological leader will depend less on Chinese actions and more on those of the United States.

The United States needs a strategy that goes beyond simply protecting its NSIB. It must also seek opportunities and build upon strengths in order to maintain a competitive advantage in innovation, development, and application. This strategy must have several lines of effort in order to cover the full scope of the NSIB. It must protect intellectual property, joint ventures, capital migration, including venture capital and private equity investment, investments in human capital, and university R&D programs.

There are four major challenges:

I. The NSIB needs to be directed, coordinated, and incentivized to win the contest for innovation.

II. The United States government has yet to fully embrace and exploit innovation in the private sector and academia.

III. The country as a whole, and the government in particular, lacks a comprehensive talent management strategy to win the technological "war for talent."

IV. The United States needs to improve its collaboration with allies and partners in order to strengthen its NSIB and the innovation capacity of those nations.

A strategy to achieve a long-lasting competitive advantage in technology and innovation must address each of these problems.

I. Directing, Coordinating, and Incentivizing the NSIB

The technologies central to the 21st-century national security landscape are changing the future of competition and conflict. These technologies include advanced computing, quantum technology, artificial intelligence (AI), autonomous capabilities, cyber, advanced wireless communications (5G and beyond), hypersonic weapons, and microelectronics, among others. In this dynamic technological environment, to achieve competitive advantage, the United States must strive to be a "first mover" whenever possible and a "fast second mover" if surprised by an opportunistic competitor. The United States must also try to protect crucial technologies by fostering their development in the United States or allied nations and providing safeguards to ensure they are secure and reliable. Given the nature of this open competition, however, the United States must also hedge against those technologies that cannot be fully protected. We should, in essence, build higher fences around fewer things.

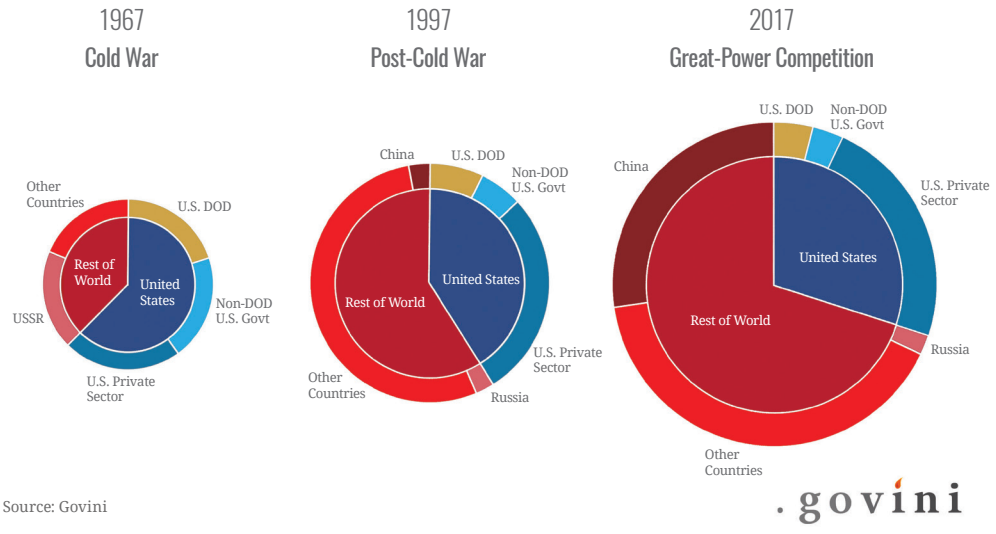
Findings:

1. The U.S. government lacks a formal structure that provides for more information sharing and collaboration among the disparate segments of the NSIB. This is the least developed and perhaps the most critical function the government can carry out.

2. The federal share of total R&D—at its lowest in over 60 years in 2018—has decreased, giving way to commercially driven R&D.[12] This trend has created both positive and negative consequences for the NSIB. On one hand, this shift has increased the total level of R&D funding in the U.S. marketplace. On the other hand, motivated by short-term performance and commercial relevance, U.S. companies have moved away from the basic research often necessary to drive generational technological advances and instead focused on shorter-term strategies tied to quarterly earnings.

   One manifestation of this trend is that today's biggest American technology companies focus more on optimizing their current products and services rather than investing in follow-on basic research—the kind that earned American companies Nobel Prizes in the past.[13]

U.S. Share of Global R&D Investment Figure 1



Source: Govini

3. Universities are a critical node of the NSIB. Their research in sensitive areas, including government-supported work on sensitive technologies, is vulnerable to foreign spying and IP theft. At the same time, the openness and attractiveness of American universities help promote scientific innovation and expand the American knowledge base.

   USG outreach to academia should be coordinated across all agencies supporting the NSIB. It should include better communication of both the threats and the opportunities for those working within the NSIB. The partnership needs to be integrated between law enforcement, counterintelligence, government labs, and policy officials.

4. USG engagement with companies and universities has helped raise awareness of the challenge but faces limitations in information-sharing and messaging.

   - Inconsistencies across USG agencies with regard to declassifying information about Chinese activity hamper the ability to bring charges against intellectual property thieves and decrease the effectiveness of warnings about the scale and effectiveness of China's efforts.

   - Even when information is declassified, the government lacks the tools and resources to disseminate the information effectively.

Recommendations:

1. Congress should authorize an interagency coordination body—the "National Security Innovation Committee"—that is responsible for enabling, developing, guiding, and safeguarding the NSIB. This entity would consolidate and elevate the existing agency lines of authority rather than create a new layer of bureaucracy. Its work should be strategic and not reactive.

    - The committee's goals would be to foster innovation in the United States or among our close allies, protect cutting-edge innovation from theft and exploitation by our strategic competitors, and establish safeguards to ensure national security applications are secure and reliable.

    - The committee would aim to facilitate common purpose and coordinated effort among the federated NSIB ecosystem, from the traditional defense and national security community to private-sector innovation centers and academia. This effort should aim to focus the NSIB ecosystem on the innovations most important to the national competition, but not in a way that dampens its greatest strength—dynamism—or introduces bureaucratic obstacles, which are the enemy of innovation.

    - The committee would clarify what the U.S. government expects of the NSIB, as the private sector elements of the ecosystem often struggle to identify sustainable technological investments in potentially vulnerable funding streams over time.

    - The committee would formally designate the critical areas in national technological competition and maintain an understanding of the dual-use technologies being developed in the NSIB.

    - Once identified, these technologies must be prioritized with long-term budgeting commitments. As such, the committee should be responsible for coordinating and submitting a unified budget analysis to Congress each year to evaluate all of the activities across the USG related to the NSIB. This analysis will bring clarity to the scope and breadth of investments in NSIB priorities and help policymakers rationalize and prioritize strategic investments.

    - The committee would have the responsibility to manage information sharing across the government and the authority to task relevant government agencies with developing and executing policies relevant to the NSIB.

    - The committee would provide a pathway for the private sector to provide input on its work.

    - Congress would include an annual reporting requirement from the committee, assessing the state of the U.S. NSIB and the government's efforts to protect it.

    - The committee should be chaired by the DOD and include representatives from other government agencies with equities related to national security innovation. Members should include the Departments of Commerce, State, and Treasury along with White House stakeholders such as the National Security Council, the Office of Science and Technology Policy, the Office of American Innovation, as well as other agencies as Congress deems appropriate. Representatives from the various agencies should be designated by the secretaries or agency heads but not below the under-secretary level.

2. The USG should expand funding for R&D and proposals for non-DOD arms of the government—e.g., the Departments of Homeland Security, Energy, and Commerce—to ensure a strong U.S.-owned and U.S.-based manufacturing center in key sectors, such as semiconductors.

    Congress should authorize a new competitive grant program to fund basic research in areas important to 21st-century competition, such as AI, autonomy, quantum technology, or advanced computing. The grant program should be administered in coordination with the DOD to fill gaps in DOD funding.

3. While not sufficient to prevail in this competition, protecting American technology and intellectual property is a critical part of the U.S. approach. Efforts to secure the supply chain, such as the recent Executive Order securing the information and telecommunications supply chain, and rules establishing cyber protection standards will be an important part of arresting Chinese IP theft and countering one of their greatest strengths. Necessary, but not sufficient, steps include the following:

    - The U.S. government should establish, maintain, and publicly release a list of academic institutions and other organizations that have a history of improper technology transfer, IP theft, or cyber espionage, or that operate under the direction of the PLA or Chinese intelligence services. The government should ban individuals who are either members of the PLA or affiliated with one or more of the organizations on this list from obtaining an F visa or J visa to the United States.

    - The State Department should strengthen Security Advisory Opinions (SAOs) for visas where there is potential for the illegal transfer of sensitive or dual-use technology. These SAOs, commonly known as Visas Mantis, should include a presumption of denial for visa applicants flagged by the State Department as potentially problematic.

      The State Department should inform companies in critical technology areas when they are recruiting or hiring individuals whose visa applications are flagged as such.

    - The USG needs new tools to combat economic and industrial espionage. One such tool could be a new interagency committee and process to allow victims of IP theft to confidentially report and provide evidence to federal agencies to consider adverse action against foreign individuals and entities the government determines have unlawfully acquired IP from a U.S. person.

4. The USG and universities should work together to protect the integrity of sensitive research projects—especially those funded by the DOD, the intelligence agencies, and the Department of Energy—including sharing best practices, bolstering university security protocols, and improving compliance. Cooperation and communication between the intelligence community, law enforcement, and universities on these issues also needs to be improved. This should include nonclassified projects that have security implications.

    - The DOD and the Intelligence Community fund unclassified but sensitive research projects at U.S. universities; however, they do not have good visibility on foreign participation in those projects. The USG should increase the required transparency of participants of this research, maintain a database of sensitive research projects, and develop a better understanding of foreign efforts to penetrate federally funded research projects.

    - Universities should strongly consider policies that limit and ultimately reject funding from companies, such as Huawei and ZTE, that are closely linked to adversarial governments seeking to gain access to sensitive research.

    - Technology produced by companies banned from the Federal Entities List should not generally be used in university research, especially research funded by the federal government.

5. The USG should pursue research partnerships with universities, similar to the existing programs with Purdue, MIT, and Georgia Tech, as a way to consolidate talent. By ensuring collaboration throughout the innovation process, sponsoring agencies can ensure efficient allocation of resources by preventing repetitive research while maximizing academic expertise. As part of these partnerships, the USG must clearly communicate the risk of espionage to universities.

6. Major defense industry associations should create new mechanisms to engage technology companies that fall outside traditional defense industry but are critical to the NSIB in their membership structure

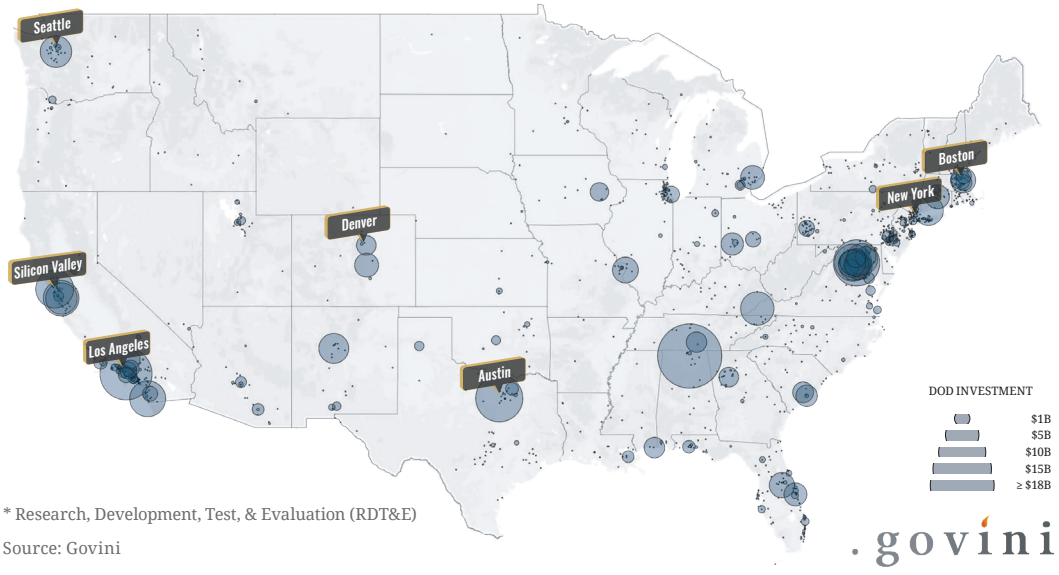
II. Optimizing and Harnessing Private-Sector Innovation

During the Cold War, the U.S. government often spearheaded innovation in advanced technology—technology that, at least initially, lacked commercial application. That paradigm has reversed. Now, the private sector generates much of the innovation in sectors critical to the NSIB, especially given the dual-use applications of many commercial technologies. As the U.S. innovation system evolved, a gulf opened between the USG and the technology industries working in areas critical to economic and national security. This divide is further exacerbated by cultural friction and the Pentagon's idiosyncratic, bureaucratic barriers to entry. Despite some success, the government has largely failed to develop a coherent innovation strategy to not only leverage high-tech developments but also stimulate them.

During the Cold War, the USG often spearheaded innovation in advanced technology—technology that, at least initially, lacked commercial application. That paradigm has reversed.

DOD RDT&E Investment vs. U.S. Tech Hubs, FY14-18

Figure 2



* Research, Development, Test, & Evaluation (RDT&E)

Source: Govini

Findings:

1. Washington has not yet fully adjusted to the new reality that national-security-relevant technologies are largely being driven by the commercial sector—not the USG, the DOD, or even the Aerospace and Defense (A&D) sector, as was true in the past.

2. There is cultural dissonance between the tech-innovation community and the DOD—but the divide is not as great as some believe, and it is reversible. Silicon Valley's most persistent concerns about working with the DOD relate to transparency and business practices. Commercial companies want to know how the government intends to use their technologies. As for business practices, if there is a viable and predictable government market for the technology with a relevant timeline, and the DOD has responsive contracting processes, capital and innovation will flow.

3. Although the federal government has made strides in bridging divides between the hubs of American innovation and Washington, DC, it has not been able fully to adapt its practices to promote or harness private-sector innovation.

    - Through programs such as the Defense Innovation Unit (DIU), the DOD has steered increased venture funding to dual-use companies. However, the DOD tends to focus on early-stage investment at the expense of mid- and late-stage investment that can enable start-ups to scale and become significant market players.

    - Beyond initial strides in narrow circumstances, the government has not shown a willingness to provide major contracts to nontraditional players. DIU remains a small element of the ecosystem, and the DOD lacks experience in integrating commercial products into its programs of record. The coin of the realm for integrating dual-use companies into the DOD ecosystem is a large program of record.

    - The DOD does not yet possess a sufficiently stable presence in Silicon Valley or approach to technology transition from strong venture and private capital-backed innovation ecosystems.

    - The USG needs to better understand how commercial technology companies are funded and incentivized, then create a structure that will motivate them to innovate and adapt technology to national security needs. That will require the DOD and other agencies to adapt to a culture that is vastly different from the traditional prime defense contractors. The primes will continue to play an important role, but commercial technology companies will be essential—and they have vastly different expectations in terms of speed, return on investment, and markets.

4. Private-sector companies are eager for government assistance in securing the building blocks of innovation, such as ensuring access to an adequate semiconductor supply chain, as well as in identifying and combatting internal and external foreign espionage. However, they are often unwilling to accept the associated government oversight that the law and regulations impose on government contractors. They would likely be more willing if the law and regulations were more transparent and easier to understand and follow.

5. With the rest of the world now gaining access to critical technologies at the same time as the United States, a key factor in technological competition is the speed with which a country can integrate path-breaking technologies into its defense systems, as well as the creativity with which it applies those systems.

6. USG policies and investment priorities cannot rely on private-sector innovation to deliver basic and applied research and early-stage development projects. Commercial development of AI is the exception and not the rule. Military-relevant technologies will continue to require R&D funding to advance needs that commercial markets will not address.

Arificially intelligent UAS, Nova built by Shield AI, one of the few startups actively pursuing contracts with the DOD.

7. The private sector's decision to fund large, long-horizon investments in R&D requires a strong intellectual property system—not just to protect IP but also to attract early-stage capital, ensure return on investment, and encourage follow-on innovation. A stronger patent system, along with the willingness to enforce licensing, will allow U.S. companies to continue to lead on innovation. That approach also plays to the competitive strengths of our system vis-à-vis China's. In recent years, efforts to weaken the U.S. patent system have diminished the ability of companies to gain and protect patents for their technologies, undercutting incentives for R&D investments and undermining innovation efforts.

8. Congress should adopt a more risk-tolerant mind-set regarding investments in national-security innovation. If political leaders want breakthrough innovation, they must show a willingness to accept failures. An NSIB that never fails is an NSIB that is not experimenting enough.

9. The congressional budget cycle is too long, and that can hamper development of critical technologies in a heated competition. New program starts are generally not allowed "out of budget cycle" to give Congress time to exercise its oversight responsibilities—but awaiting the completion of a full budget cycle might take 18 months or more, depending on when a new idea emerges.

10. Policymakers can encourage sought-after innovation by establishing clear criteria, signaling it to the commercial sector, and demonstrating the existence of a marketplace through adequate purchasing levels. Additionally, necessary trust must be built where promised procurements and timelines can withstand leadership and administration transitions.

Recommendations:

1. The DOD should implement a variety of reforms to the way it does business, with the goal of acculturating its technology acquisition to the more risk-positive nature of the NSIB and driving incentives for private-sector actors to participate more purposefully and robustly in the NSIB.

    - The DOD should make use of its alternative acquisition pathways to award contracts as part of programs of record to companies to ensure a sustainable funding profile. Although one-off R&D funding has a role to play in the innovation ecosystem, it alone will not adequately integrate new technologies into military platforms, nor will it give investors confidence that there is a real market to justify later-stage venture investment.

    - The DOD should measure progress in contracts awarded, total dollars awarded, and speed of procurement, focusing on writing fewer, larger checks both as a way to leverage key emerging technologies and as a signal to investors.

    - The DOD should overhaul software acquisitions to move away from requirements lists to iterative capabilities and maximize the use of commercial standards for interoperability.

    - The A&D sector should be incentivized to increase its investment in dual-use companies. Unlike other large industries, the A&D sector has traditionally not been a leader in corporate venture investing. A&D companies can benefit from placing "bets" on innovative start-ups, deliver much-needed capital during later-stage venture rounds, and help companies overcome the USG barriers to entry—but they need to be encouraged by the government to do so. The DOD should open up fast-track and other preferred acquisition programs to A&D companies with strong venture programs.

    - Dual-use start-up and venture capital sectors should be more open to investment from "strategics." Waiting for the DOD to place big bets on new entrants should not be the only path toward integrating start-ups.

- Programs such as DIU, Defense Digital Service (DDS), and Hacking for Defense (H4D) should serve as models for ways to remove obstacles to collaboration between the USG and business and academic components of the NSIB.

2. Congress should redefine a "new start," with innovation in mind to "fast track" exciting new technological opportunities within the congressional budget cycle. The authorizing committees should make a special effort to identify projects that must start on an expedited basis and flag the appropriations committees about the importance of permitting such programs out of cycle.

3. DIU rotations in innovation centers should be longer, allowing DOD representatives in Silicon Valley and other technology innovation hubs more time to establish the relationships and social networks that are necessary for long-term success. The DIU should also continue to hire from those ecosystems with rapid hiring authorities.

4. Congress should provide sustained, predictable, increased funding for the DIU, including fully funding its National Security Innovation Capital fund.

5. The USG should reverse recent efforts to diminish the strength of the U.S. intellectual property system, providing companies with clear pathways to obtain patents and offering the predictability, certainty, and enforceability necessary to inventive endeavors.

   Changes in federal law could also better enable the private sector to recoup financial losses resulting from IP theft. Congress should consider amending the Foreign Sovereign Immunities Act to include a long-arm statute establishing U.S. jurisdiction over Chinese firms operating in the United States.

6. Congress should establish a more generous R&D tax credit, increasing the "Alternative Simplified Credit" above the current 14 percent, to incentivize investment in the crucial, early-stage basic and applied research likely to drive innovations key to the NSIB.

   The current U.S. R&D tax credit is much more limited than those of U.S. competitors and ranks only 25th among the 35 member-states of the Organization for Economic Cooperation and Development (OECD).

7. The USG must ensure that companies under the direction of the Chinese Communist Party do not obtain a near-monopoly on 5G wireless technology. Congress should codify the Executive Order on domestic telecommunication supply chain security and consider enshrining Huawei's position on the Commerce Department's entity list. Ensuring American technological leadership should be the guidepost of any actions in this regard. The administration should, therefore, clarify that interaction with listed entities in international standard-setting bodies is permissible.

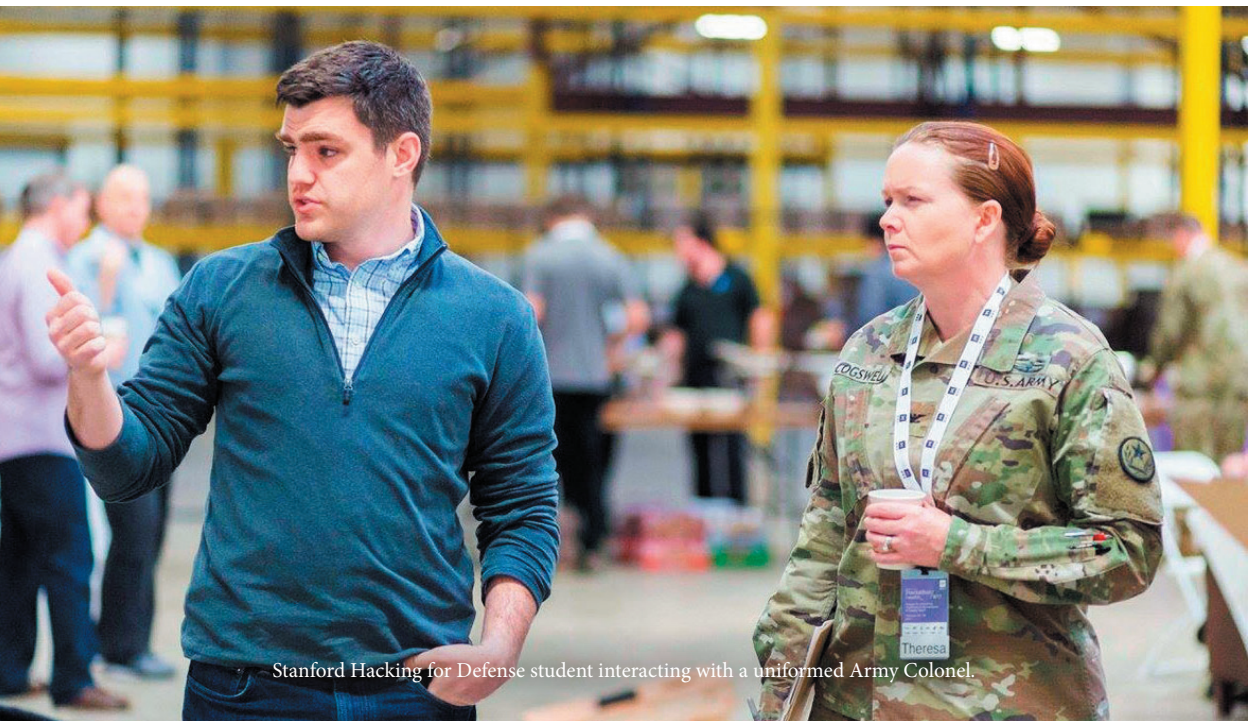
   Winning the race for 5G means doing more than playing defense. The United States must help support non-Huawei 5G bids abroad in concert with like-minded allies. One option could be a 5G Development Fund that would extend lines of credit, similar to the BUILD Act, to strategic partners seeking to develop 5G wireless networks. The United States does not have to block Huawei everywhere abroad, but it must ensure there is a large-enough market for non-Huawei equipment to keep Western-aligned competitors in business.

Two Success Stories: DDS and H4D

The Task Force was particularly impressed with two programs working to harness tech innovation—and innovators—to solve problems: the Defense Digital Service and Hacking for Defense. The former approaches the problem from the inside out; the latter from the outside in. Both programs are shaking up the DOD enterprise by:

- Reinterpreting and reimagining mission challenges in useful ways;
- Bringing the best civilian tech talent to bear on behalf of national security;
- Breaking down cultural barriers, pulling the tech and defense worlds together, and creating a recruitment pool of tech talent for the future;
- Leveraging the knowledge of private tech leaders to seek out the best problem solvers for particular challenges;
- Introducing the DOD to other parts of the NSIB ecosystem (e.g., the academy, tech entrepreneurs);
- Acclimating our warfighters to thinking from a tech point of view about solving problems; and
- Blazing the trail in navigating existing DOD processes to bring new innovation and energy to the department.

While scaling such programs will prove difficult, it is important to acknowledge the successes of programs already tackling the problems we want the NSIB to solve. Programs like these, which operate at the grassroots level, are the best way to coordinate the NSIB ecosystem without straitjacketing its independence and dynamism.



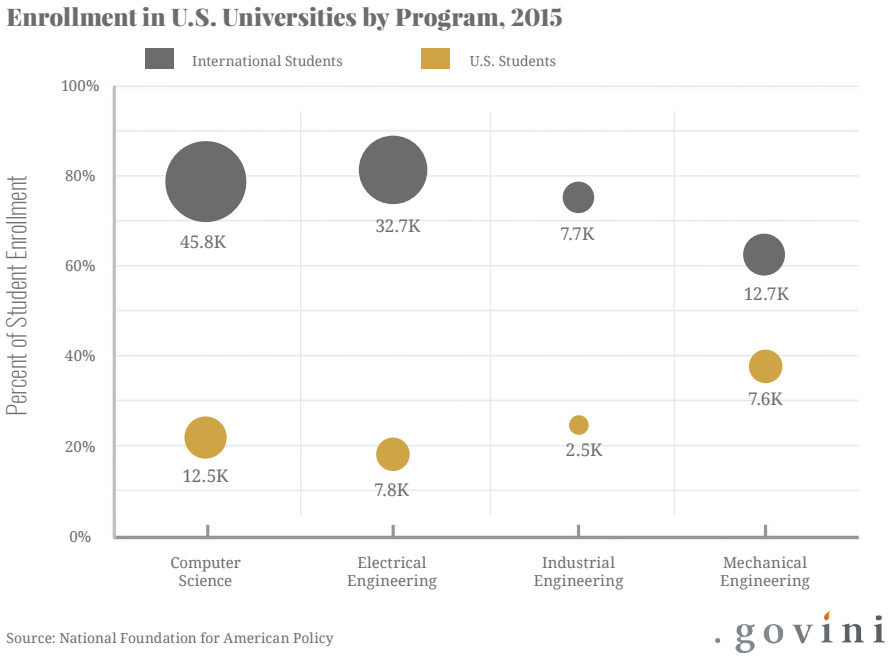
Stanford Hacking for Defense student interacting with a uniformed Army Colonel.

III. Winning the War for Talent

As much as emerging technologies will define future conflict, the war for talent will likely play the central role in the outcome of long-term technological competition. The NSIB struggles to attract, recruit, and retain a workforce willing and able to tackle tough challenges and find innovative solutions. Universities are confronting a dearth in American talent generation and retention, and much of that shortfall is filled with foreign students, a large share of them from China.

The ability of American universities to attract foreign students and scholars has many benefits, including spurring innovation, but the United States must do more to develop and retain the human capital it produces. Currently, the majority of foreign students who obtain masters and doctorate degrees from U.S. universities return home instead of entering the U.S. workforce. Private-sector companies working with the USG face a lack of workforce talent eligible for government clearances to work on national security projects. The government, meanwhile, struggles to attract and retain computer engineering and software talent, as well as to develop such talent internally. The effect is a brain drain that is working against our national interest—the opposite of the one we benefited from in the 20th century.

Figure 3

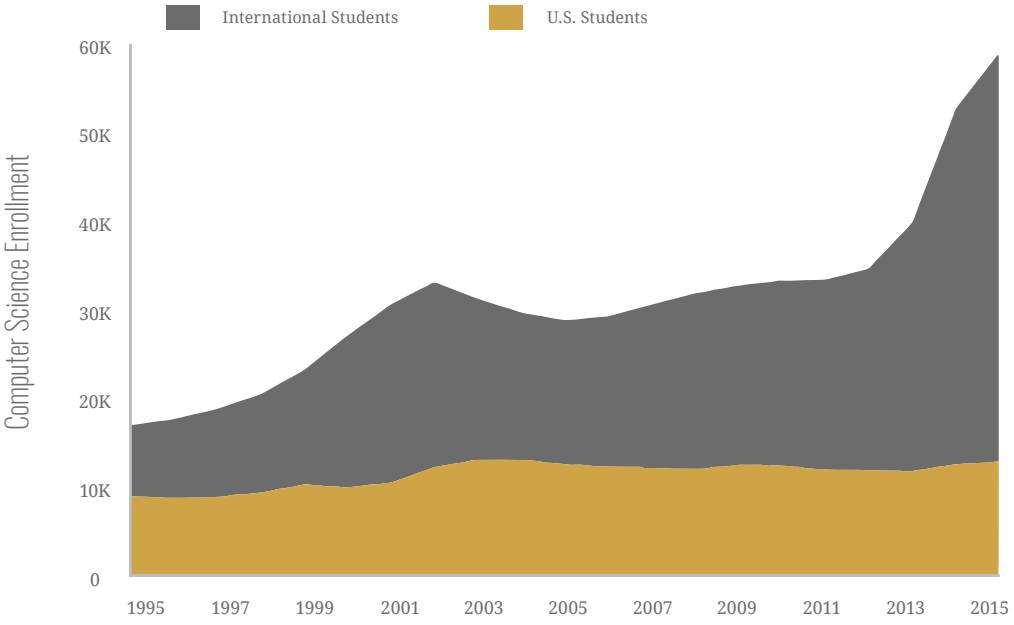


Findings:

1. Unlike its reaction after the "Sputnik moment," the USG now seems content to let market forces determine the pull for national technical talent. These forces are unlikely to be sufficient in the face of a Chinese national plan to grow the talent pool necessary for a concerted technological competition.

2. Universities are struggling to build and maintain the talent pipeline critical to sustaining the NSIB. Universities rely on foreign students, a large fraction of which are Chinese, to field graduate-level engineering programs. Some 80 percent of graduate students in technical fields like engineering and computer science are foreign nationals.[14]

Computer Science Enrollment in U.S. Universities, 1995-2015 Figure 4



Source: National Foundation for American Policy

. govini

This talent gap is partially due to the fact that private-sector companies attract American students graduating from bachelor's programs with lucrative salaries and immediate offers of employment following graduation, causing them to forgo graduate degrees.

3. There is a huge diversity gap in STEM—and, even more significantly, among patent holders. This is also an opportunity to focus on leveraging presently untapped talent into technical fields for advanced degrees and R&D.

4. U.S. immigration policies further impede the war for talent, often requiring foreign students graduating with high-demand technical degrees to return to their home countries rather than providing pathways for them to stay and contribute to the U.S. NSIB.

5. Chinese students, in particular, are pursuing technical degrees in far greater numbers than American students, both at home and abroad—and most of those who earn degrees abroad are returning to China afterward for employment.[15]

6. Although some national-security-related research and development does require doctoral-level education, much does not. Targeted investments and incentives that are aligned with desired educational end-states can all contribute to improvements in the NSIB workforce.

7. Initiatives such as the Defense Digital Service succeed by providing flexible pathways for government service doing meaningful work, and they offer an opportunity for augmenting the government NSIB workforce.

8. The DOD does not sufficiently value the potential contributions of software engineers, with few, if any, software engineers having authority to act and maneuver on critical issues within the department. Outside of DDS, there are limited opportunities for software engineers to perform meaningful work. They are often relegated to Cyber Command, where they cannot develop software and often face long wait times for security clearances.

Recommendations:

1. Congress should authorize the creation of a new national civilian "STEM Corps" modeled after the Reserve Officers' Training Corps and the National Guard. Students would be selected through a competitive process to receive full tuition to attend public universities and study specified disciplines related to national security technology. In return for accepting the scholarship, graduates would commit to spending several years serving in either the "active" or "reserve" STEM Corps, working within a component of the NSIB ecosystem.

   The "active" component of the STEM Corps would include graduates working full-time in designated government and DOD billets. The "reserve" component would work two days each month and 14 days each summer with government agencies or DOD offices. The reserves would provide flexible, short-term pathways of service for those working in the private sector.

2. Congress should create a "National Security Innovation Base Visa" that would encourage appropriately vetted, highly skilled workers to come to the United States or foreign national students graduating with relevant degrees to stay in the United States. This approach would incentivize them to contribute their education and talents to the long-term benefit of the NSIB.

   The NSIB Visa should target relevant fields, such as AI, automation, cybersecurity, and various dual-use technologies. It could be used to draw global talent to work across the sectors of the NSIB ecosystem—from private companies and university faculties to the Departments of Defense and Energy—with appropriate but expedited vetting of applicants pursuant to the level of clearance needed for particular positions.

3. Congress and the Executive Branch should pursue incentives for introducing computer literacy and coding training at early stages of education. Congress should increase financial incentives for industry to champion early STEM education programs.

   Military bases should increase community outreach programs to students in cybersecurity, computer science, and STEM to encourage participation in internship opportunities with the services, exposing talented students to the mission of the DOD. Currently, outreach programs at bases vary, and additional outreach would be mutually beneficial for the military and students.

4. In addition to expanding programs such as DDS and the DOD public-private talent exchange program, which promote relatively brief rotations in and out of government, the USG and the private sector should create longer-term, flexible-pathway programs allowing participants to move between public service and the private sector. Over time, rotating people through meaningful assignments will create the kind of personal relationships and cultural awareness that draws the whole ecosystem together without the kind of top-down coercion that inhibits creativity.

   The DDS should provide an annual briefing to Congress to provide recommendations for navigating the system of hiring computer scientists, as well as mitigating educational and structural IT challenges within the DOD.

5. The USG should maintain security clearances for cleared individuals transitioning from government to the innovation sector to help ease their return to government service, either full-time or part-time, later in their careers.

6. The USG should evaluate whether security clearance holders should, upon leaving government service, be able to work at companies like Huawei or Kaspersky, which are financially backed by adversarial governments.

7. The military services and Cyber Command should be given authority to structure special recruitment packages with maximum flexibility on length of service, training requirements, rank, and compensation for personnel with high-value technical skills. While the DOD may never be able to compete with the private sector on compensation alone, flexibility to waive employment requirements, including clearances, will help—along with creating more awareness of the value of meaningful public service.

8. The DOD should prioritize developing career paths for active-duty military computer scientists and software engineers to ensure they are able to continue advancing in rank throughout their military service.

IV. Mobilizing Allies and Partners

The ongoing global technological competition is largely between democratic and authoritarian states, whose exploitation of technology reflects their own values. The United States does not possess a monopoly on ideas, technology, or talent. The United States needs to partner with its allies on innovation just as it does on collective security; those partnerships will be force-multipliers for the NSIB. The value chain for the technologies critical to the NSIB is inherently global—and strengthening the U.S. NSIB will require incentivizing and leveraging commercial technology not just in the United States but also among its trusted allies and partners. One way to offset China's increasing military–civil fusion is to access and exploit global commercial research and development. The United States already possesses a legal and regulatory structure to facilitate cooperation on innovation among its closest allies. The National Technology and Industrial Base (NTIB), which includes Canada, the United Kingdom, and Australia, mandates that the DOD seek to integrate the industrial bases among these nations.[16] Expanding the functionality of the NTIB and exploring supplementary policies and regulations are critical steps in strengthening the NSIB.

The United States needs to partner with its allies on innovation just as it does on collective security; those partnerships will be force-multipliers for the NSIB.

The Cost of Compliance

The Task Force learned that businesses in the United Kingdom—one of our closest allies—spend more than $500 million each year just to navigate the compliance obligations of doing business with the United States, particularly with trade controls. That equates to roughly 1 percent of the UK's annual defense budget.

Although we recognize the importance of responsible acquisition and trade policy, this imbalance can harm U.S. and allied readiness. Our allies' spending on compliance should shift to spending on capacity and capability.

Findings:

1. Shifting from a mind-set of U.S. technological dominance—in which America generates breakthrough innovation and parcels it out carefully as needed—to a mind-set of U.S.-led cooperation with its allies

on leveraging commercial innovation will require a cultural shift. That shift will depend on recognizing the nature of the competition. It will also depend on viewing technology and capability transfers not just as security risks but also as potential assets.

2. As China continues to grow and implement its fusion strategy, the United States will need to leverage alliances and partnerships to compete over the long term. Allied contributions have been brought to bear in the military arena (e.g., through NATO and Major Non-NATO Allies), and policymakers must determine how to utilize it in the broader NSIB context, as well.

   Washington and its close allies and partners collectively boast one of the strongest and most innovative markets in the world. Greater integration will expand access to friendly nations' contributions, and thereby empower the NSIB.

3. Any reform initiatives, whether in the United States or abroad, will face significant bureaucratic challenges. Countries have strong reasons to support their domestic industries and to protect their sensitive innovations.

4. The USG has also rightly raised concerns about sources of trusted foreign capital and controlling investments in critical technologies. The USG recently enacted the Foreign Investment Risk Review Modernization Act (FIRRMA), which transformed the jurisdiction, authority, and operation of the Committee on Foreign Investment in the United States (CFIUS) to address these and related concerns.

5. The NTIB model has inherent potential strengths, and an expanded NTIB can strengthen the U.S. innovation base.

   - According to a recent analysis, the NTIB "offers the opportunity to immediately add 40 percent in capacity to the U.S. industrial base" by providing "additional scale and [filling] some of the manufacturing holes that currently exist."[17]

   - The countries within the NTIB are close allies. All are part of the Five Eyes intelligence-sharing alliance, and all but Australia are members of NATO. They boast dynamic economies and robust commercial innovation bases. Existing efforts to integrate their innovation bases, such as NTIB and the International Traffic in Arms (ITAR) exemptions granted to Canada, have streamlined some areas of cooperation and technology sharing. NTIB countries are pursuing further means of collaboration. Further exemptions beyond the current limited Canadian exemption would allow for collaboration without the fear that ITAR will be attached to each instance of U.S. participation.

6. Much of the technological development critical to the NSIB is occurring within but also beyond NTIB nations. U.S. allies are pursuing significant R&D in specialized areas, from AI and cyber to space and anti-access area denial. The principle of comparative advantage offers a road map to thoughtful and effective collaboration.

   - NATO remains a foundational military alliance and represents an important forum for NSIB cooperation as well.

   - Key partners both inside and outside NATO, including Norway, Israel, Sweden, South Korea, and Japan, have all made substantial gains in specialized technologies. However, in some cases, they hesitate or struggle to cooperate with the United States due to its onerous regulatory and licensing system that leaves them feeling unwelcome as partners in our defense ecosystem.

7. The U.S. export-control system, a legacy of the Cold War, limits the industrial and commercial base available to the USG, discourages allied governments and commercial entities from accessing the American marketplace, and hinders cross-border collaboration among scientists and engineers. In effect, U.S. export controls impose burdensome restrictions on technologies widely available to American adversaries while dis-incentivizing R&D and commercial-market cooperation with allies.

Recommendations:

1. Congress should authorize a new international framework—the "Partnership for a Strong Innovation Base"—to allow the NSIB to capitalize on the capabilities of the United States' most trusted allies. The framework should be designed to give the United States access to cutting-edge technology from close allies and to encourage those countries to make robust investments in military capabilities to enhance the common defense.

    - The partnership should allow trusted allies and partners to benefit from a regulatory fast track for their key investments. The regulatory approach for these investments and partners should be one of presumptive openness. Burdensome acquisition rules and trade controls should apply only when specifically required.

    - Congress should shape priorities for areas of cooperation based on the needs of U.S. national security, where international cooperation has some precedent and offers key advantages.

    - Eligibility for accession to the partnership should be based on key criteria, including

        - the record of commitment to investment in national defense as defined by the level of spending on national defense and defense-related infrastructure;

        - the level of investment and cooperation with the United States, particularly within the U.S. defense industrial base;

        - the value to military interoperability;

        - the country's degree of defense and security cooperation with the United States; and

        - the existence and extent of existing security agreements and reciprocal defense agreements.

    - Consistent with the need to safeguard U.S. national security, certain laws—including foreign investment and industrial security—could be applied in a more discerning way, rather than being waived altogether. For example, partnership benefits could include favorable presumptions or prioritized reviews, building on provisions of law that grant favorable treatment to NTIB members.

2. The United States should sharpen and focus existing authorities to enable U.S. companies and the USG to leverage opportunities generated by companies in allied nations.

    - As an initial matter, Congress should consider applying the Canadian ITAR exemption to Australia and the United Kingdom as part of the NTIB integration process.

    - It should also broaden that exemption to apply to a greater range of technologies, since the current exemption excludes certain critical technologies, such as cybersecurity. Such measures would allow innovative technologies and defense materials to move across NTIB borders without licenses, creating a zone of enhanced collaboration for key technologies.

3. Congress should streamline technological exchange by making program-wide licenses available, such that companies and governments need not seek individual licenses for each component part of a particular technology or at each stage of project development. A coordinated, strategic framework for R&D cooperation would allow U.S. allies to drive innovation toward common goals.

4. As it considers how to strengthen the NTIB and expand partnerships with other nations, the USG must also consider the kinds of technologies to prioritize, and with whom.

- High-priority technologies could include AI; space; cyber; quantum; integrated intelligence, surveillance, and reconnaissance (ISR); autonomous systems; and hypersonic technologies. By focusing on particular areas of cooperation, policymakers should identify the specific expertise allies and partners have to offer and create special mechanisms to facilitate cooperation in those areas while avoiding a costly and time-consuming attempt to engage in wholesale export control and acquisition reform.

- The United States and its allies can also consider how to pool their resources to incentivize NSIB innovation. The Five Eyes nations could launch a "Five Eyes Grand Challenge," modeled after DARPA's highly successful series. The challenge would be open to engineering teams and entrepreneurs from all five countries and focus on developing solutions to a common military operational problem.[18]

5. The U.S. intelligence community should work toward more transparency with allies, such as the Five Eyes—particularly when it comes to creating standards and norms. Not only would this reduce the barriers on sharing technology and working on projects as a coalition, it would also strengthen offensive deterrence capabilities. Instead of hoping our allies continue to trust our method of attribution of cyberattacks, working in conjunction with them will provide greater gravity in an

Conclusion

An ascendant, technologically advanced China poses a threat not just to U.S. security but also to the values of freedom and democracy that have shaped the world for more than a half century.

The contest for innovation between the United States and China will turn largely on which system innovates more effectively over time. If it is the Chinese system, then China may unseat America as the primary global power, supplant the technological dominance of the United States and its allies, and reshape the world in its authoritarian image. That need not and should not be the result—but preventing it will require swift and decisive action to strengthen the National Security Innovation Base.

Rolling back Chinese high-tech authoritarian ambitions will require a strong, dynamic, cohesive, and secure NSIB. Though the American private sector has delivered transformational technologies in the past, today's NSIB will be incapable, in its current state, of producing the national security innovations needed for the United States to outcompete China. To respond to China's technological challenge, enhance the American way of life, and protect the national security, the NSIB ecosystem must produce cutting-edge technologies more often and more reliably than China's centralized, government-led innovation system.

Our strategy should be confident, opportunistic, and entrepreneurial—but also clear-eyed and pragmatic. Closer collaboration and coordination among the groups that comprise the NSIB is vital, as is building the pipeline of talented minds dedicated to sharpening America's innovative edge. Leaders must work to eliminate the cultural disconnect and distrust between the public and private sectors. The recommendations in this report provide a path to countering China and its existential threat to U.S. national interests, global stability, and our way of life.

The Task Force calls on all Americans and allies of freedom to take from this report a sense of urgency. The United States, and its partners around the world, have huge reservoirs of strength and invention that, taken together, are more than sufficient to decide the outcome—if the leaders of our innovation ecosystem will work together to harness the power of technology in the service of a free and peaceful world.

Sources

[1] The President of the United States, National Security Strategy (2017): 29, accessed November 25, 2019, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; U.S. Department of Defense, National Defense Strategy (2018): 3, accessed November 25, 2019, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[2] Samuel Bendett and Elsa B. Kania, "Chinese and Russian Defense Innovation, with American Characteristics?—Military Innovation, Commercial Technologies, and Great Power Competition," The Bridge (August 2, 2018), accessed November 25, 2019, https://thestrategybridge.org/the-bridge/2018/8/2/chinese-and-russian-defense-innovation-with-american-characteristics-military-innovation-commercial-technologies-and-great-power-competition.

[3] See, e.g., Elsa B. Kania, "In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate," The Bridge (August 27, 2019), accessed November 25, 2019, https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate.

[4] Kania, "In Military-Civil Fusion."

[5] Update to the IP Commission Report, The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy (2017): 1, accessed November 25, 2019, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.

[6] Jim Zarroli, "Judge Orders Chinese Wind-Turbine Maker to Pay $59 Million for Stealing Trade Secrets," NPR, July 6, 2018, accessed November 25, 2019, https://www.npr.org/2018/07/06/626683457/judge-orders-chinese-wind-turbine-maker-to-pay-59-million-for-stealing-trade-sec.

[7] See, e.g., James A. Lewis, Center for Strategic and International Studies, Emerging Technologies and Managing the Risk of Tech Transfer to China (September 4, 2019): 16, accessed November 25, 2019, https://www.csis.org/analysis/emerging-technologies-and-managing-risk-tech-transfer-china.

[8] Christian Brose, "The New Revolution in Military Affairs: War's Sci-Fi Future," Foreign Affairs (May/June 2019), accessed November 25, 2019, https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs.

[9] Michael Brown and Pavneet Singh, Defense Innovation Unit Experimental, China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation (January 2018): 3, accessed November 25, 2019, DIUx Study on China's Technology Transfer Strategy - Jan 2018.pdf.

[10] Dustin Volz, "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets," The Wall Street Journal, March 5, 2019, accessed November 25, 2019, https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800.

[11] See, e.g., Alex Joske, "Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities" (2018), accessed November 25, 2019, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-10/Picking%20flowers%2C%20making%20honey_0.pdf?H5sGNaWXqMgTG_2F2yZTQwDw6OyNfH.u.

[12] Caleb Foote and Robert D. Atkinson, Information Technology & Innovation Foundation, "Federal Support for R&D Continues Its Ignominious Slide" (August 12, 2019), accessed November 25, 2019, https://itif.org/publications/2019/08/12/federal-support-rd-continues-its-ignominious-slide.

[13] J. John Wu, Information Technology & Innovation Foundation, Why U.S. Business R&D Is Not as Strong as It Appears (June 2018): 7, accessed November 25, 2019, http://www2.itif.org/2018-us-business-rd.pdf.

[14] Nick Wingfield, "The Disappearing American Grad Student," The New York Times, November 3, 2017, accessed November 25, 2019, https://www.nytimes.com/2017/11/03/education/edlife/american-graduate-student-stem.html.

[15] Youyou Zhou, "Chinese Students Increasingly Return Home After Studying Abroad," Quartz (July 29, 2018), accessed November 25, 2019, https://qz.com/1342525/chinese-students-increasingly-return-home-after-studying-abroad/.

[16] National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 881, accessed November 25, 2019, https://www.congress.gov/114/crpt/hrpt840/CRPT-114hrpt840.pdf.

[17] William Greenwalt, Atlantic Council, Leveraging the National Technology Industrial Base to Address Great Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies (April 21, 2019), accessed November 25, 2019, https://issuu.com/atlanticcouncil/docs/leveraging_the_national_technology_.

[18] Daniel Kliman and Brendan Thomas-Noone, Defense One, How the Five Eyes Can Harness Commercial Innovation (July 25, 2018), accessed November 25, 2019, https://www.defenseone.com/ideas/2018/07/how-five-eyes-can-harness-commercial-innovation/150040/.

Dedicated to the preservation and promotion of Ronald Reagan's legacy of inspired freedom.

The Ronald Reagan Presidential Foundation and Institute (RRPFI) is the non-profit, non- partisan organization established by President Reagan whose mission is to promote his legacy by convening, educating and engaging people around the world in his core principles of freedom, economic opportunity, global democracy and national pride. The Ronald Reagan Institute in Washington, DC – an entity of RRPFI – promotes President Reagan's ideals, vision, and leadership example for the benefit of generations to come through substantive, issue- driven forums, academic and young professional programming, and scholarly work. The Reagan Foundation sustains the Ronald Reagan Presidential Library and Museum. At the dedication of the Reagan Library in November 1991, President Reagan defined its purpose by describing it as a living institution where scholars interpret the past and policy makers debate the future.

BOARD OF TRUSTEES

Frederick J. Ryan, Jr.*
Chairman

Catherine G. Busch *
Secretary

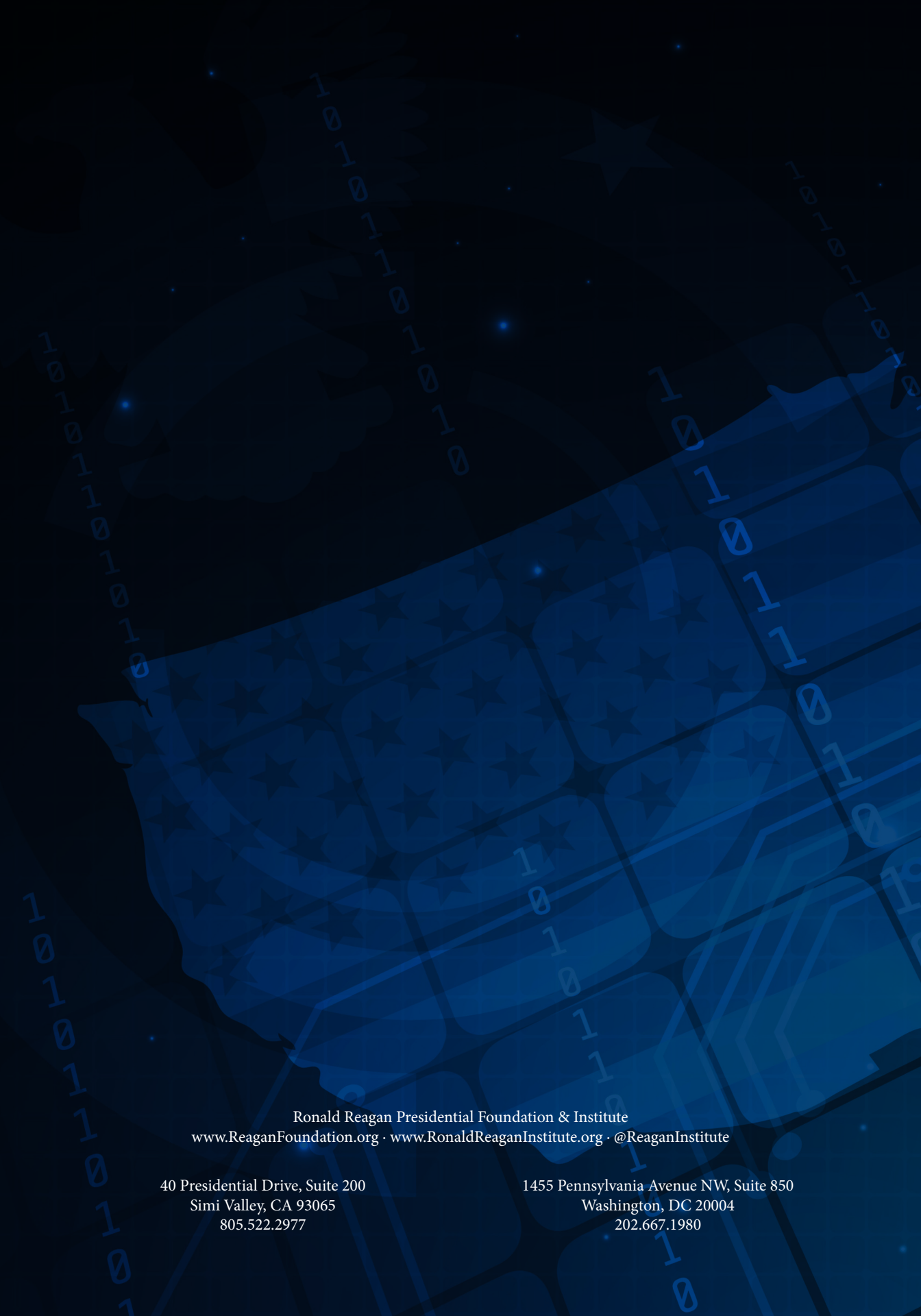
John F. W. Roger *
Treasurer

John D. Heubusch
Executive Director

***Lifetime Members**

Rick J. Caruso
Michael P. Castine
Lodwrick M. Cook*
Robert Day
Steve Forbes
Bradford M. Freeman
Rudolph W. Giuliani
Jeffery R. Immelt
Ann McLaughlin Korologos
Andrew J. Littlefair
Susan R. McCaw

Rupert Murdoch
Peggy Noonan
Theodore B. Olson
Gerald L. Parsky
Jim Pattison
Paul D. Ryan
George P. Shultz*
Ben C. Sutton, Jr.
Robert H. Tuttle*
Pete Wilson



Ronald Reagan Presidential Foundation & Institute
www.ReaganFoundation.org · www.RonaldReaganInstitute.org · @ReaganInstitute

40 Presidential Drive, Suite 200
Simi Valley, CA 93065
805.522.2977

1455 Pennsylvania Avenue NW, Suite 850
Washington, DC 20004
202.667.1980