Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

LEVERAGING THE NATIONAL TECHNOLOGY INDUSTRIAL BASE TO ADDRESS GREAT-POWER COMPETITION:

The Imperative to Integrate Industrial Capabilities of Close Allies

William Greenwalt

LEVERAGING THE NATIONAL TECHNOLOGY INDUSTRIAL BASE TO ADDRESS GREAT-POWER COMPETITION:

The Imperative to Integrate Industrial Capabilities of Close Allies

William Greenwalt

ISBN-13: 978-1-61977-586-2

April 2019

Contents

Executive Summary

In US law, the national technology and industrial base (NTIB) comprises the industrial bases of the United States and three of its closest historical allies (Australia, Canada, and the United Kingdom). Canada was included when the original NTIB was established in 1994, while Australia and the United Kingdom were added by Congress in 2016. The current NTIB expansion has corresponded with a changing threat and technology environment, in which non-defense and global actors are now leading technology innovation. This new threat and technology environment will require a different type of NTIB to support future defense-industrial planning and execution.

This study is an attempt to begin a discussion on what a new NTIB should look like, and how Congress and the administration can pursue policies that can prepare the United States and its allies to compete in this new environment. Through a series of visits, interviews, and discussions with US, Australian, Canadian, and UK industry and government officials, defense experts, and academic researchers, the barriers to increased defense cooperation at the industrial level between the NTIB countries were assessed. The actions needed to address those barriers were identified, and the outcome of this report begins to describe those specific legal, regulatory, and policy changes that are necessary to advance industrial cooperation within the NTIB.

Three large trends argue for the need to use greater NTIB integration to leverage the capabilities of US allies and the commercial marketplace as a means of addressing US national security needs. The first is a return of great-power competition. China is a profoundly different potential adversary than the old Soviet Union and will require a different approach than what was successful in the Cold War. The second trend is the US military has allowed its technological dominance to atrophy. Adversaries and allies have begun to achieve parity in defense capabilities, and in some cases are moving beyond the United States, while the commercial marketplace is leading in innovation in many areas of relevance to national security. The privatization of research and development (R&D) has led to a technological leveling on a global scale, at the same time that new threats to the United States are emerging. Technological reinvention of capabilities that already exist and are available to US adversaries is a losing strategy in an era where global and commercial R&D far outstrip what the Department of Defense (DoD) can afford.

Finally, the continuing erosion of US technological dominance and the reemergence of a great-power competition are revealing the current US export-control system to be not only inadequate with respect to the United States' closest allies but, as a whole, detrimental to the national security of the United States. This national security threat from the current export-control process manifests itself in three ways. First, there is a residual US focus on Cold War technologies that have long since proliferated to US adversaries, leaving allies with the burden of compliance. Changing business practices, such as the outsourcing of logistics and maintenance activities to the private sector, have exacerbated this compliance burden. Second, export contamination—or the so-called "ITAR taint"—and the extraterritorial application of US export-control laws limit the industrial base available to US defense programs, and has incentivized both allies and the commercial market to develop their own solutions that deliberately avoid US technology and persons. The third is the emerging possibility that other countries will incorporate the most intrusive parts of US export-control systems into their systems. As foreign technologies become increasingly important, this mirror imaging of export-control process around US standards could eventually have a dramatic impact on US operations by placing limitations on the use of foreign technology.

The US ability to go it alone in all aspects of national defense-industrial policy is rapidly eroding. Establishing procedures within a trusted group of allies, such as within the NTIB, could allow the United States to pursue greater technology cooperation and transfer approaches in a more secure environment that could be helpful in expanding the industrial base, both commercially and with more traditional defense entities. It is with this goal in mind that Congress expanded the number of countries belonging to the NTIB and also its focus on civil-military integration to address the globalization and commercialization of military-relevant technologies. Meeting the statutory requirement of reducing "the barriers to the seamless integration between the persons and organizations that comprise the National Technology and Industrial Base" will not be easy, as embedded processes and a cultural aversion

to changing what worked in the Cold War will stand in the way. [1]

As a means of achieving this seamless integration, twenty-two specific legislative options to enhance the NTIB have been identified, to implement four broad recommendations.

The four study recommendations address: governance; technology-transfer reform; acquisition reform; and the further expansion of the industrial base. The ultimate goal is a step-by-step process leading to a harmonized NTIB defense free-trade area for goods, services, and—most importantly—ideas and research, within a defined, trusted community that will work to maintain the technology dominance of the United States and its closest allies. Each of these four categories of recommendations is supported by a discussion of specific legal or regulatory proposals.

Recommendation #1: Establish a governing body of NTIB members to address harmonization of industrial-base issues.

To achieve effective NTIB integration, an integrated quadrilateral governance structure will need to be established. This high-level group, comprising senior officials of the NTIB countries, would address harmonizing policies and practices in areas including regulating direct foreign investment, technology transfer, research and development, supply chain, and communications and information-technology infrastructure security. This group would approximate an equivalent to the "Five Eyes" intelligence-alliance format for the industrial base, but with a more formal governance structure. The intelligence basis of the "Five Eyes" arrangement, however, is directly relevant to the NTIB, which needs to be as much about protection of technology from adversaries as about sharing it between allies. Intelligence sharing within the NTIB is also highly relevant to decision-making on future technology investment.

Recommendation #2: Harmonize technology-transfer laws, regulations, policies, and practices to establish an integrated defense-industrial base.

The export-control regime within the NTIB will need to be dramatically reset. A new technology-control system, based on a trusted community of industrial partners, should be established and tested within the NTIB to incentivize advanced research and development, as well as greater defense cooperation to meet the new security environment. A first step would require the US administration to apply the Canadian International Trafficking in Arms Regulation (ITAR) exemption to the UK and Australia, but also significantly broaden this exemption to address issues of ITAR contamination or taint (the use of controlled US knowledge at the research-and-development stage that applies to a product or service forever) and extraterritorial application of US export-control regulations and laws that have outlived their usefulness as guiding principles—at least among close allies. Additional legislative options address supply-chain transfers, program licensing, the foreign military-sales program, and past defense trade treaties with the UK and Australia.

Recommendation #3: To the maximum extent practicable, limit socioeconomic and acquisition process barriers to cooperation

NTIB expansion is a key component of US acquisition-reform efforts that originated in the 2016 and 2017 National Defense Authorization Acts. The reciprocal elimination of socioeconomic mandates, and a harmonization of acquisition processes within the NTIB, would further improve the integration of the four countries' industrial bases. These socioeconomic barriers to participation include domestic source restrictions, small-business preferences or set-asides, and offset agreements.

Recommendation #4: NTIB industrial-base approaches should serve as a test bed for innovations in international cooperation, be applied on a case-by-case basis to other close allies, and further civil-military integration between Silicon Valley and the Department of Defense.[2]

Once implemented and tested within the NTIB, many of these reforms could potentially be advanced on a case-by-case/country-by-country manner to some of the United States' other closest allies—those that have both a reciprocal defense-procurement-and-acquisition policy memorandum of understanding and a security-of-supply agreement with the United States. In addition, lessons learned from the NTIB experience could be applied to accessing emerging technologies within a trusted community, to better incorporate defense programs with globalized commercial firms

1 Section 881, National Defense Authorization Act for Fiscal Year 2017.

2 While the term "Silicon Valley" is a geographical description of the information-technology hub that grew up in the San Jose/San Francisco corridor in the United States, in this study it will be used to stand-in for the broader innovation culture of nontraditional firms and a venture capital ecosystem that have now planted innovation hubs in many other geographical areas in the United States, and elsewhere in the NTIB.

based in such places as Silicon Valley, Cambridge in the UK, Waterloo, Canada, and other high-tech innovation clusters. Many of the same barriers to working with the DoD that apply to the commercial information-technology industry also apply to the NTIB countries and the closest US allies. The primary lesson learned from this effort is that Cold War management institutions, such as the ITAR and the US acquisition system, are now limiting the DoD's access to some of the best technologies in the world. If the United States wants to compete in the future, it will need to change those institutions.

Introduction

The legal construct underpinning defense-industrial base strategy, analysis, and planning in the United States is contained in chapter 148 of title 10, United States Code (see Appendix A for specific statutory language). The secretary of defense is required by law to develop and maintain a defense-industrial strategy for the national technology and industrial base (NTIB) that is integrated with the National Security Strategy required by the National Security Act of 1947, as well as the National Defense Strategy, which implements the National Security Strategy and is required by section 113(g) of title 10, United States Code. It must also be supported by the budget as outlined in the Future Years Defense Plan, as required by section 221 of title 10, United States Code. It is no coincidence that national security strategy, industrial policy, and defense budgets are integrated and intertwined by law.

What is probably not as well known is that the legal definition of the NTIB, established in 1992, applies to persons and organizations engaged in research, development, production, integration, services, or information technology activities not only in the United States, but in Canada as well. In section 881 of the 2017 National Defense Authorization Act (see Appendix B) the United Kingdom and Australia were included in the definition of the NTIB. Congress made it clear in section 881 that the seamless integration of the industrial bases of the United States, Canada, Australia, and the UK is needed to address growing threats.

As Congress no doubt understood, seamless integration faces many implementation challenges. Despite countervailing forces encouraging disaggregation, progress was made through the NTIB mechanism to maintain some level of the integration achieved during the Cold War between the US and Canadian defense-industrial bases. The US-Canada NTIB was created in a period of significant defense drawdown and conversion in the immediate aftermath of the Cold War—but also in recognition that, since World War II, defense-industrial capacity was grounded in a historical cross-border integration between industrial plants and firms in the United States and Canada. The NTIB between the two countries was already a reality in practice at the time it was recognized in law, and the compelling issue was how to keep it together. For the last three decades, a key industrial policy concern has been how to preserve those minimal remaining defense-industrial capabilities as a hedge against future needs as the defense supply base underwent dramatic consolidation and reduction in capacity. The US-Canadian NTIB and the standalone US defense-industrial base are shadows of their former selves, but still a vital foundation of capabilities to build upon.[3]

However, implementing an effective NTIB in today's environment will be even more challenging. The NTIB needs to radically change from what has existed since the end of the Cold War. The NTIB expansion also reflects the significant current level of integration between the defense industries of the four member nations. Paralleling the position between the United States and Canada in the 1990s, today most major US defense firms (such as Boeing, Lockheed Martin, General Dynamics, Raytheon, and Northrop Grumman) have facilities in both the UK and Australia, while major international players like BAE Systems and Rolls Royce now consider the United States a domestic market after years of inward investment.

The NTIB expansion was a complementary part of the targeted-acquisition reforms in the 2016 and 2017 National Defense Authorization Acts, which were designed to remove barriers to accessing new sources of innovation. With these reforms, Congress recognized the potential return of great-power competition, which was subsequently validated in the 2018 National Security Strategy and National Defense Strategy documents.[4] Thus, to be integrated into national security and national defense strategies—and to address the strategic imperative of that great-power competition—the NTIB of the 2020s will need to be profoundly different from the NTIB of the past. This will include a greater need to partner on new innovation, rather than focus on maintaining and protecting

3 For a discussion of the vulnerabilities that have crept into the US defense-industrial base and the NTIB over the years, from lack of investment and new defense programs, see "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States" (report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806), September 2018.

4 "National Security Strategy of the United States," US Department of Defense, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; "2018 National Defense Strategy of the United States of America," US Department of Defense, January 2018, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

a backward-looking industrial capability as a hedge against a future undefined threat. That threat has arrived, and the industrial base needs to undergo significant transformation to meet it.

The Compelling Case for a Robust Implementation of the NTIB

Three large trends argue for the need to use greater NTIB integration as a means of addressing US national security needs. The first is a return of great-power competition in a form vastly different from the Cold War competition with the Soviet Union. The second is the US military allowing its technological dominance, gained during the so-called "second offset" of technology developed in the 1970s and visibly displayed in the first Gulf War, to atrophy.[5] The United States and its allies appear to be at risk of suffering a reverse "offset"—for example, through Chinese and Russian development of hypersonic missiles. The final trend is that the current export-control system, also established in the 1970s and designed to protect that technological dominance, is now a threat to US national security, as it severely constrains US technological advancement while doing little to hold back great-power adversaries.

The Rise of Great-Power Competition

The United States faces a new threat environment that has not been seen since the height of the Cold War. In fact, this threat is more dangerous and complicated, with a resurgent military and nuclear power in Russia, an emerging superpower in China, and medium-sized powers such as Iran and North Korea growing their military and nuclear capabilities. The 2018 National Security Strategy and National Defense Strategy documents are unlike those of the recent past, which were severely budget-constrained and primarily focused on antiterrorism operations. US strategy now significantly recognizes the current threat, and outlines the new challenges facing the United States in an emerging era of great-power competition.

Strategy documents are one thing; doing what is necessary to implement a strategy is something else. A significant effort will be required to mobilize and sufficiently prepare for any major great-power conflict. Still, the primary purpose of US and allied military and foreign policy over the past seventy years has been to prevent any such conflict. During the recent decades of US and allied hegemony, it could be argued that a significant lesson from the Cold War has been forgotten: that military capability is required not just to fight a war, but to prevent it. If US and allied military capability cannot respond to current challenges quickly enough, a potential great-power adversary may no longer feel sufficiently deterred from taking steps that could bring about conflict. So, technological and doctrinal innovation is as critical for deterrence as it is for warfighting.

Gearing up for a great-power conflict would be daunting enough on its own, but the United States still needs to address the legacies of its post-9/11 conflicts as it mobilizes in preparation for an even greater potential struggle. As the global threat increases, the US military is essentially trying to do five things at once. Each requires new levels of innovation from an expanded industrial base, different acquisition approaches, and a required defense budget that will significantly outpace what is likely to be achieved.

First, the United States must maintain current legacy operations around the globe. While specific deployments, such as in Syria and Afghanistan, may be under debate and subject to change, the threat from terrorist entities is unlikely to go away in the near future. Addressing these threats requires continual industrial innovations that can be deployed quickly (in no more than two years) under the rapid-acquisition approaches that were first developed at US Special Operations Command (SOCOM), and used to support operations in Afghanistan and Iraq. Secondly, there is a practical need to focus on readiness, training, and repairing the equipment that has worn out during the operations of the last two decades. This second priority area alone could take up much of any currently envisioned defense-budget increase, but would at least return US forces to a level able to fight with their current technology and systems. The problem is that many of those systems—while useful in counterterrorism operations—will become increasingly outdated in a great-power conflict.

Next, the United States needs to modernize at scale. This third effort requires expanding current production lines and mobilizing capability, to hedge against

5 It seems that, with the change in administrations, many have stopped using the terms "first, second, and third offsets." Still, it is hard to find a better terminology for at least the first two periods of intense US defense-technological innovation that occurred in the 1950s and early 1960s, along with missile and space-reconnaissance developments and, in the 1970s, with advancements in stealth, precision guidance, and geolocation. Whether the United States can actually implement a third offset—based on artificial intelligence, autonomy, quantum computing, data analytics, and other emerging technologies—remains to be seen. But, if it can, it could rival the two previous periods of technology innovation.

inevitable losses in any great-power war. It also requires fast incremental innovation to enhance capability of existing systems, as demonstrated by the Special Capabilities Office, and for the services to rapidly acquire new capabilities as envisioned under the Section 804 rapid-fielding authority. The fourth, simultaneous objective is disruptive innovation. Section 804 operational-prototyping authorities and other transaction-contracting authorities can help move disruptive systems into the hands of the warfighter faster. This means not only experimenting with operational prototypes, but also providing new realities on the ground that complicate Chinese and Russian military planning.[6]

Finally, the fifth objective is the need for business reform to free up resources to support operations, improve readiness, mobilize, and disrupt, as—absent a full-scale ware—there will likely never be enough money to do all of this. However, by that time it will be too late, given mobilization timelines and a historical lag of two years or longer to get industrial capability to frontline troops. Former US Secretary of Defense Donald Rumsfeld was unfortunately correct when he said, "You go to war with the army you have, not the army you might want or wish to have at a later time."[7] The lesson the United States continues to relearn is that it should use peacetime to address as many things as possible that will cause problems on the future battlefield, meaning it has to spend real money during that time. Peacetime business processes—whether they support acquisition, requirements, budget, finance, or technology and security control—are often designed with objectives other than immediately supporting the warfighter. These processes add costs, and also limit the industrial base to those able to comply with them, limiting the technology choices available to the Pentagon. All of these business processes need to be put on more of a wartime footing.[8]

The difficulty with this problem set is that the current, dedicated US defense-industrial base and the US acquisition system are not prepared for a great-power war, nor the innovation necessary to compete in all five things the United States must do to meet its national security needs. Nor has it geared up to deliver the significant innovation in capability and doctrinal development to deliver a sufficient deterrent effect to prevent that war in the first place.

For the last seventeen years, the United States has been equipped to conduct current operations against insurgencies and terrorism in the arc of instability running through Central Asia to Northern Africa. Because of the constant threat of budget sequestration, wars have been fought on the cheap and readiness levels have fallen. Modernization is being conducted at non-economic order-of-production levels. Disruptive innovation has been practically nonexistent, as research funding has historically stopped at the 6.3, or advanced-technology, development level, leaving most innovations stuck in the so-called "valley of death." Prototyping, or 6.4, funding has been difficult, if not impossible, to obtain. Science and technology (S&T) communities are addicted to the existing peacetime way of doing research by doling out funds in single million-dollar increments, and the budget reflects that. Business reform is further constrained by the inability to address the costs of socioeconomic requirements placed on the Pentagon by Congress and past administrations. Large-scale technological and business-process disruption will be needed to meet the great-power threat. While Congress took the first step in passing new-acquisition reforms in 2015 and 2016, much more needs to be done to implement these reforms and reform other business practices. Finally, and perhaps most importantly, since the end of the Cold War the United States and its allies seem to have subconsciously forgotten the requirements of deterrence, as there was no great-power rival to deter. With the resurrection of great-power challenges, the atrophy of US and allied capabilities during that period now appears to be a huge vulnerability.

The NTIB is an integral part of Congress' recent acquisition-reform efforts, and will need to adapt to support each of these five objectives. It needs to be flexible enough to bring scientists and engineers together across borders—in many cases, within the same companies that have facilities in each of the NTIB countries. The NTIB needs to be ramped up to support research and development, rapid incremental modernization, and disruptive innovation, and to bring in new sources

6 Section 804 of the 2016 National Defense Authorization Act provides new acquisition flexibilities in exchange for forcing the Department of Defense to deploy capability through rapid fielding, or an operational prototype in less than five years from initiation of the program. While this authority has huge potential to change the balance of power, and each military service is currently experimenting with this authority, it remains to be seen how successful implementation will ultimately be.

7 Eric Schmitt, "Iraq-Bound Troops Confront Rumsfeld Over Lack of Armor," *New York Times*, December 8, 2004, https://www.nytimes.com/2004/12/08/international/middleeast/iraqbound-troops-confront-rumsfeld-over-lack-of.html.

8 The Section 809 panel took up this call to return acquisition policy to a wartime footing in its most recent *Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations* 3, January 2019.

of business innovation to support higher readiness levels, improved maintenance, and better management. That is currently not happening, as managers, scientists, and engineers within the NTIB are precluded by US law and regulation from even talking to one another without first seeking prior authorization from the US administration. This stymies, rather than fosters, innovation by imposing cost and time penalties on information sharing that a potential innovator may be unwilling to incur. That has taken on greater importance because of recent trends in technology development and diffusion.

The Loss of Technological Dominance

The Ronald Reagan defense buildup of the 1980s produced the systems developed earlier in the 1970s. For the most part, the US military still relies on these technologies, such as precision strike, advanced geo-location, and stealth. For more than thirty years, the DoD has been able to take an innovation holiday, because of the absence of a near-peer adversary to deter. These 1970s technologies were marginally improved over the years within an acquisition system that primarily rewarded compliance and process, rather than innovation. Still, slow and wasteful business processes, and a sclerotic acquisition system that resulted in incremental improvements to these Reagan-era systems, may not have mattered as long as the United States maintained its technological dominance. The government-unique industrial base that has coalesced around these processes can be extremely inefficient, but can still meet US needs as long as no one is chasing the United States. Keeping allies at arm's length and putting up barriers to working together can also work if the United States leads in all technologies; it really doesn't need allies if it can do everything itself.[9] All of this has now changed, probably forever. The primary threat no longer drives around in the desert in a Toyota Land Cruiser, but will be delivered in a hypersonic missile. The United States has lost its technological dominance on many levels and will continue to do so at a rapid pace, but the culture and business processes predicated on the United States always having technological dominance have not adjusted to this fact.

The United States' loss of technological dominance has emerged in three areas. US adversaries, the commercial market, and even allies are all leapfrogging US capabilities. This erosion of US dominance occurred because the rest of the world didn't stand still over the last three decades. First, Russia and China have been able, over time, to replicate the defense-unique aspects of US military power, through either dedicated research or the stealing and replicating of US technology. Parity has been achieved at many levels, and the United States is now falling behind its adversaries in niche areas where they have made significant investments. This is highly dangerous. Not only has US technological superiority prevented great-power conflict during this time, but that advantage was overwhelming, and seen to be so. Parity and niche-area advantages on the part of potential adversaries, or even the perception that they exist, may be sufficient for deterrence to fail.

What adversaries have not adopted is the current US acquisition system that takes decades to field systems. Retired Admiral Gary Roughead, the co-chair of the Commission on the National Defense Strategy of the United States, recently stated: "The Chinese have adopted our rapid innovation [model] and we have adopted the communist model of how we process new capabilities in our system."[10] US adversaries are pursuing rapid prototyping and deployment of new technologies in short increments. This is similar to how Silicon Valley brings out new versions of products and, not surprisingly, also similar to how the United States used to develop weapon systems in the 1950s and early 1960s—including the first intercontinental ballistic missiles (ICBMs) and reconnaissance satellites, as well as helicopters, missiles, planes, and ground vehicles. It is likely that adversaries will move to production in large quantities of the technology that provides the most advantage to change the balance of power, whether in the South China Sea or the Baltics. There is also a focus on exploiting US weaknesses in cyber and electronic warfare through anti-access areal denial strategies, which is to be expected.

The second level on the road to technological inferiority is that the commercial market is now ahead of the US military. Nothing better illustrates the US military's loss of technological dominance than its relationship

9 Perversely, it can be argued that the inability to access US technology has directly driven the poor cost-effectiveness of many allies' national-procurement decisions, the inefficient sustainment of duplicate industrial capabilities, and the loss of US exports, with all of the economic and employment consequences that entails. Allied burden sharing might be significantly better today had the United States been less restrictive in its willingness to share its technology with some of its closest allies, or at least sell to them, over the past three decades.

10 "Commission Co-chair Bashes Pentagon Acquisition System," *National Defense*, November 28, 2018, http://www.nationaldefensemagazine.org/articles/2018/11/28/commission-report-cochair-bashes-pentagon-acquisition-system.

with Silicon Valley. The DoD is already behind the commercial market in several of the technologies identified in the National Defense Strategy as keys to future defense applications. These include artificial intelligence (AI) and machine learning, software development, data analytics, autonomy and robotics, and biotechnology. Due to the globalization and proliferation of these dual-use technologies—which will be even more important as future force multipliers and differentiators—they are now, and will continue to be, available to US adversaries and allies alike.

While the commercial market is now ahead of the military, the DoD has not made it easy for firms that want to innovate on its behalf. It is remarkable that the United States continues to put up barriers to the commercial market over unwarranted fears of excess profits and the desire to control intellectual property. All of this stands in contrast to its adversaries, which have no qualms about tapping into non-traditional firms and technologies. Despite the US inventing the term in the 1990s, China's understanding of the importance of civil-military integration of the defense-industrial base, and President Xi Jinping's role in leading advocacy for it, contrasts starkly with US actions and leadership.

One would think the United States would embrace this market. But, despite limited—and not yet completely successful—outreaches to Silicon Valley through the Defense Innovation Unit, the Pentagon's acquisition bureaucracy has been outright antagonistic to commercial providers of solutions. This results in favoring cost-type contract programs with traditional contractors, rather than fixed-price commercial contracts, and locking in government-unique terms and conditions rather than commercial ones. The situation has not improved, despite new laws to remove barriers to commercial innovation. Things have gotten so bad that those few commercial companies that have tried to sell solutions to the DoD—such as SpaceX, Palantir, and AGI—have been forced to sue the department to get their commercial products considered. Meanwhile, the Pentagon spends its limited research-and-development (R&D) dollars on what can only be called developmental-reinvention efforts, with traditional members of the military-industrial complex, to replicate what is already available in the commercial marketplace. So, as its adversaries race ahead, taking advantage of advances in the commercial market, the United States continues to operate as if it is still the mid-1970s—when DoD military-unique technology was dominant, and Silicon Valley was still taking its first steps to usher in the PC revolution.

The third area where the United States is falling behind is in the technological relationship with its allies. Due to the globalization and proliferation of dual-use technology, many US allies have experimented with civil-military integration and new commercial ways of doing business—precisely because they have had fewer resources to spend on defense than the United States has had. They have also maintained steady R&D in certain defense-unique areas in which the United States stopped investing. As a result, they have developed expertise in specialized areas of defense-unique capabilities, in which they are now ahead of the United States. The NTIB countries—and also many NATO allies such as Norway and France, as well as non-NATO allies such as Sweden, Israel, South Korea, and Japan—have seen significant advances in these niche technology areas, but are hesitant about truly cooperating with the United States, given the next trend.

Export Controls as a Threat to National Security

This final trend is intimately tied to the first two, the major disincentive to allied and commercial defense cooperation, and the most significant barrier to real NTIB integration. The US technology-control system is designed for an era of US technological dominance that no longer exists. The export-control mechanisms, which were designed to maintain US technological dominance developed at the height of the Cold War and protect the advances of state-sponsored R&D, have lost their relevance in an era where global commercial R&D investment outstrips military R&D. The legacy export-control system not only impedes economic security, but also poses a threat to US national security.

This national security threat manifests itself in three ways. First, there is a residual, perhaps obsessive, US focus on Cold War technologies that have long since proliferated to US adversaries, leaving allies with the burden of compliance. Changing business practices, such as the outsourcing of logistics and maintenance activities to the private sector, have exacerbated this compliance burden. Second, export contamination—or the so-called "ITAR taint"—and the extraterritorial application of US export-control laws limit the industrial base available to US defense programs, and has incentivized both allies and the commercial market to develop their own solutions that deliberately avoid US technology and persons. The third is the emerging possibility that other countries will learn the wrong lessons from the US experience, and will incorporate the most intrusive parts of US export-control systems into their systems. As foreign technologies become increasingly important, this mirror imaging of export-control process around US standards could eventually have a dramatic impact on US operations.

Cold War Legacies

The US export-control system has become increasingly backward looking. It is designed to control things that have already been developed; this seems logical enough as the initial basis of control, but then takes the view that any US content must be the dominant technology that triggers controls. This becomes an issue when any US person becomes involved in technology development, however superficially. This could become even more apparent and problematic in the current attempt to control "emerging technologies," which may incorrectly assume that US industry, research, and investment still independently dominate these technologies. The system goes out of its way to be nondiscriminatory, controlling goods and services on an equal basis for both US allies and potential enemies. An arms embargo may keep China from ever being granted a license to buy US weapons, but the real impact is felt by US allies who may be granted a license to gain access to US content after six to nine months of excruciating, bureaucratic process. Potential enemies or competitors would never apply for a license, so they either need to steal, indigenously develop their own technology, or buy from Russia or China. Thus, US export controls are really about allocating technology to US allies, and keeping it out of the hands of third- and fourth-tier countries that do not yet have the capability to develop it themselves. As a result, the US system has largely defaulted into a process of arms-sales transactions to the developing world, and a bureaucratic nightmare for close allies and industry.

One can assume that those in charge of implementing the US export-control system truly believe that they are adding value through their actions. However, allies would not be entirely wrong if they thought of the current US export-control system as the means by which a fading power that still thinks itself dominant grants favors to others. When the United States is dominant, these countries might complain about this treatment, but can be ignored, as they still need US technology. That has been the case since 1945, but is increasingly changing. When US dominance slips, the rationale for the whole system comes tumbling down, which has become clearer in the last decade.

There are no doubt still technology areas in which the United States is still dominant, and is fearful that less careful allies would be one-way conveyers of technology to Russia, China, or Iran. Still, after thirty years of relatively low-level, incremental technological advancement, the threat to the United States has increased to the point where more and more of what is controlled is already in the hands of Russia and China, and could be increasingly developed by most US allies. There is no differentiation in the US system between advancements that maintain the US edge against its enemies, and what has already proliferated into the defense market.[11]

As a result, allies have already been forced to develop their own indigenous technology, because of restrictions placed on US technology and the need to have a competitive solution. For other systems, where technology is widely available, it would just take time and effort to do so. Ideally, it would be easier to simply buy from the United States, but that does not always work under the current system. The current US comparative advantage is the basis for its arms-sales industry—which, while robust, is selling a fraction of what it probably could, due to the US arms-transfer process. That means fewer American jobs, lost economies of scale, revenue for rival suppliers, and reduced US influence.

Still, NTIB countries have it better than most. The difference between the closest US allies, such as those within the NTIB, and other allies is the former will likely always be granted an export license after six to nine months.[12] Why is such a long process needed? As much of what the US is controlling was first developed in the 1960s and 1970s, and is widely available in foreign versions, allies should question US reasons for controls. When the UK and other close allies begin to believe that they are being treated in the same manner as Niger or Chad, for technologies that Russia and China have had for decades and that US allies could make on their own if they had to, it is reasonable to question the system's logic.

But, first, how did things get to this point? The imperative to control military goods has a long pedigree, with both military and foreign policy aspects. The current US export-control system goes back to the rise of the Cold War and the recognition of the Soviet Union as an adversary. This began with the Export Control Act of 1949, which prohibited the transfer of anything of military or strategic significance to communist countries.

11 Despite the intention of export-control reform (ECR) in the last administration to focus the ITAR on US "crown jewels," and transfer other items to the Commerce Department, under a system that is more flexible as regards US allies, this review found no appreciable differences from this reform effort that practically reduced the burden of cooperation with allies.

12 As will be discussed later, there will be some technologies that are denied or only allowed to be transferred under certain conditions—even to close US allies, such as those in the NTIB—but the key point here is to make a distinction between the vast majority of routine transfers and, importantly, the discussions necessary for ongoing research cooperation and development.

Export controls further evolved with the passage of the Arms Export Control Act of 1976 and the establishment of the current ITAR to implement the act. Each of the premises of the ITAR made perfect policy sense in the mid-1970s. The United States was in competition with a country that was completely separated from the economies of the West. The United States and the Soviet Union competed at the level of state-run national laboratories, and directed research-and-development programs within highly secretive and closed-off industrial units. Soviet espionage was highly active in Western Europe, with a large focus on attempting to steal technology and bring it back to the "motherland." In this environment, it made sense for the United States to be careful about what it gave its allies.

Prior to 1975, the US and Soviet governments were the engines of global innovation. Commercial-technology advances were still in their early stages, and allies' industrial bases were still weak. Thirty years after the end of World War II, NATO allies still played a minor role in the scientific and engineering community of the Alliance. The United States was still the "Arsenal of Democracy," and its allies were generally not competing with the United States in terms of military technology. US commercial research-and-development expenditures per year had yet to surpass US government R&D, and did not do so until the 1980s. The US military was just beginning to develop technologies, such as stealth and the global positioning system (GPS), that would establish US conventional forces' dominance. Under this system of governmental control and dominance, a system of bureaucratic control of technology was needed to keep the Soviet Union from taking advantage of US government research.

All roads at the time led to Washington, DC, and technology transfer and control would be a mechanism not only for the United States to protect NATO's military dominance, but, increasingly, to be a method of foreign policy control. For better or worse, this foreign policy aspect would eventually became predominant when the Department of State and the corresponding Foreign Affairs Committees in Congress—rather than the Department of Defense and the Armed Services Committees—gained primary, if not absolute, control over-export control issues.

While US export controls began as a tool to maintain US technological dominance, one could argue that is no longer its primary mission. A process of control grew up around those Cold War technologies, which the United States wanted to keep out of the hands of the Soviet Union and its clients. However, this process, like many bureaucratic systems, has evolved into a rigid, one-size-fits-all monstrosity. The question is why, and one logical answer is the State Department found in this system a means of power and influence to bring allies into line and control their military operations. Rather than trust allies, the United States instituted a system requiring them to check with Washington first, before deploying forces dependent on US technology.[13] It is no wonder that these allies are chafing to remove US content from their militaries, to get out from under that control.

It was not US allies yearning to be free that began to undermine the US export-control model, but the rise of commercial R&D. This began in force in the 1980s, and the subsequent globalization of that R&D in the 2000s began to undermine the state-directed, defense-developmental model. Globalization and the passage of time have eroded US technological dominance and—as outlined in the most recent Commission on National Defense Strategy—in many cases, the United States is already behind. Potential adversaries have been catching up due to the so-called "peace dividend" and the US focus on combatting terrorism.

As the United States has fallen behind technologically and pursued incremental improvements in its legacy weapon systems, the heart of what it controls is Cold War-era technology. That technology may still be lethal, and beyond the technological capabilities of many countries, but it is increasingly questionable, after three decades of global technological advances and proliferation, that it is beyond the capabilities of many NATO and major non-NATO US allies. Yet, because the export-control process does not differentiate upfront between allies and potential export markets, or the availability of capabilities, the system takes excessive time to approve licenses. This delay has operational impacts, and delays allies' abilities to develop their own systems or partner with the United States. While most, if not all, of the license requests for NTIB countries are eventually approved, the time delay has an operational and industrial impact that is not justified, and is a source of unnecessary irritation with US allies and the US forces that fight alongside them.

13 The US State Department would argue that it, indeed, does allow a government license to receive US equipment to deploy its military using that equipment, but it then insists on requiring licenses to maintain that equipment once deployed. This is a distinction without a difference. It is of no practical value in a conflict, or operating together as an alliance, when all military equipment needs constant maintenance, particularly when deployed.

What is the ITAR "Taint"?

The aforementioned irritation could probably be manageable if US controls with NTIB allies were conducted solely at the end-item level. If the United States decided to sell a C-130 to the UK or Australia—and if one export license covered the export of the item, the corresponding spare parts and maintenance, and the ability to use and deploy this item—this could be a reasonable system. The United States would sell an item, and then allow the buyer to use and maintain the system in the way it sees fit. This end-item level of control is the system that US allies have in place under their export-control regimes. In this example, the UK could then use that C-130 to conduct operations, usually alongside the United States, and maintain the aircraft through its supply chain. The reality is it can't. While an export-control system that takes six months to a year to get a license for a US end item would still probably be a paperwork exercise, at least it would only involve one piece of paper. It could also be initiated before the system is built, having only a potentially delaying impact on production schedules.

This is not the case because of export-control contamination and the extraterritoriality application of US export-control laws. Export contamination has been called the "ITAR taint," but the idea is actually much broader, as contamination can also occur in the Foreign Military Sales (FMS) program and the Commerce Department export-control system. These concepts have limited allies' abilities to operate their defense systems efficiently, or to fight side by side with the United States. They have also put up huge barriers to cooperation with the United States, encouraged the development of non-US solutions, incentivized the holding back of technology by US allies, and opened up a huge potential rift with the commercial sector, which prevents the United States from accessing certain commercial technology.

The criteria for US control are key. The United States is not unique in controlling items at the end-item level, as well as at the major-component and subcomponent levels. The United States is also not unique in controlling certain identified technologies behind controlled hardware; this is basic to all nonproliferation regimes. The United States is unique in controlling the "casual" release or "deemed export" of technology—in other words, any knowledge associated with a controlled item—to foreign persons. This is the source of the ITAR taint, but export contamination can also apply to Commerce Department controls for items under its jurisdiction. The trigger to initiate US export control is the transfer of controlled knowledge from a US person to a non-US person. This sounds reasonable, but the definition and application of that knowledge have grown to ridiculous proportions. That knowledge can be in a blueprint, a repair manual, or an enterprise resource planning (ERP) system. It can be released via conversation, email, or a technician's access to the ERP system. The larger the application of controlled technology, the larger the potential knowledge-point applications.

Thus, items are controlled not only at the end-item, component, subcomponent, and technology levels, but at the knowledge point or information related to the item. Any discussion with a foreign national—by phone, by email, or in a meeting of engineers having coffee—risks divulging information, in what is called a "deemed export." As US export controls have evolved, the system has moved from controlling tangible end items of military equipment, to components, to technology, to knowledge of that technology, to any service done to that equipment. The thousands of licenses now required—each with specific provisions for how to implement the transfer of US goods, services, or knowledge—have created a tsunami of bureaucracy within defense companies and NATO allies. This bureaucracy has a significant direct cost in the numbers of employees, information systems, compliance checks, legal opinions, and other processes that any company (or foreign government) handling ITAR material needs to have in place. In a 2017 report, the UK government estimated this direct cost of ITAR compliance for UK companies at more than $500 million annually.[14] All of that money is spent on servicing US government regulations, not on getting capability into the hands of the warfighter. These direct costs, however, pale in comparison to the indirect cost on limiting innovation.

The ensnaring net of US export controls gets worse when it begins to "taint" a product, whether foreign or commercial. The trigger to initiate US export controls is the transfer of any knowledge, usually—but not always—through the expenditure of US defense R&D dollars at some point in the supply chain. However, they can also be triggered by a discussion with a US citizen about something that one might think only has a tangential link to a military product, which ultimately becomes the source of the so-called "ITAR taint." For example, within one company operating in the both the United States and the UK, a UK engineer had an offhand discussion with his US counterpart about some significant advances in UK commercial technology.

14 "Final Report for the British Embassy in Washington D.C on U.S. Export Compliance Costs," Baker Donelson, March 28, 2017.

That discussion, while not highly significant to the advancement of the product, "tainted" the ability of the UK portion of the firm to ever use that technology without getting a US export-control license.[15] Once a technology is tainted by exposure to a US person, this taint never goes away. Many foreign and US companies that choose to help the US military and jointly contribute to US capability find that they lose control of the ability to sell, and even use, their technology without going to the State Department for a license. If anything within a system is controlled under the ITAR, that means the final product and, often, the entire system is subject to ITAR controls.

Many US commercial firms that were interviewed for this study looked at the prospect of an ITAR taint as an original-sin problem. Controlled US knowledge at the research-and-development stage taints the product forever. Thus, US commercial firms are wary of, if not downright hostile to, doing any research that might have a military application. They will do whatever it takes to commercialize their research first, by selling it in the global marketplace. For the same reason, foreign companies don't want any US participation, even having a US engineer on a project. Through the mechanism of the State Department, the US military closed itself off from the global innovation market.

The ITAR taint becomes magnified by one of the most problematic aspect of the US export-control system—the concept of transfers and retransfers. Unlike other nations, the United States continues to follow its content and knowledge throughout the lifecycle of their use. This could be somewhat manageable with a focus on a systems end item, but anything associated with the United States needs to be tracked. This means any movement of an ITAR-controlled item or knowledge that has been tainted with US content (however defined) within a foreign country's supply chain, and was not approved ahead of time, requires a new export license. Also, because of the threat and severity of export fines—even when export transfers may already be authorized—US firms are reluctant to act without further clarification from the US government, which leads to unnecessary delays in the use of US items.

Transfers and retransfers of defense items, services, or knowledge have become a huge issue with US allies, even without a proposal to sell technology to third countries. This is significant because the US export-control system has not caught up with how weapon systems are now maintained. Maintenance used to be a government-only function, but the United States and most of its major allies have found it is cheaper to outsource this work to the private sector for many defense systems. This means foreign contractors could ideally shift in and out of a supply chain on a daily basis, just as they do in the United States for US systems. However, every time there is a change in a contracting relationship, this is defined as a retransfer, requiring a new license and a corresponding six-to-nine-month delay in implementation while waiting for State Department approval.

This has real, practical implications for US allies in the NTIB. For example, all equipment bought through the Foreign Military Sales (FMS) program requires submission of a separate retransfer request to the State Department after delivery, to enable items to be passed to contractors for insertion on a country's platforms. One can only imagine the paperwork and delays necessary to outfit a ship such as the UK's Queen Elizabeth Class aircraft carrier. The need to seek separate approval for supply under FMS, and then a retransfer to contractors under ITAR, adds a layer of delaying bureaucracy that adds unnecessary time, risk, and cost to allies' most important programs. And if the Royal Navy wanted that same ship to use systems originally bought for use on other vessels it owns—and/or wanted to incorporate items bought directly under ITAR, rather than FMS—those are completely separate processes, managed by different US agencies. The United States should decide whether to cooperate upfront on programs such the UK's carrier program, and then do everything it takes to make it happen. Otherwise, it is just wasting the purchasing power of its allies on red tape and contractors being paid to wait around.

In a similar example, as part of a routine upgrade, an FMS-sourced sonar system was to be installed in a UK submarine. The contractor employed was a highly controlled and security-cleared entity previously approved to handle other US-origin equipment. But, the UK still had to seek specific State Department approval to allow the contractor to perform some fairly basic work. Again, months went by waiting for a license that just added cost and risk to an ally's military capability. The UK government and the contractor had long been seen as trustworthy, but could do nothing until their application cleared a desk in Washington.

Just as the United States has done on a number of occasions, the UK made an efficiency decision to contract out the management of its defense warehouses. Of course,

15 Interview with author. This conversation had the effect of undermining this company's competitiveness, and likely led to a significant potential loss of commercial sales.

this decision was punished by a smothering bureaucracy emanating from the United States. Similar issues will undoubtedly arise as information is contracted out from government-controlled data centers to the private-sector "cloud." One former participant involved in the warehouse transaction described what happened next:

> "In order to enable the selected contractor to handle US-controlled items we had to obtain an extensive and comprehensive approval from two separate US Departments, via different staffing routes, even though there would be no change of ownership of the stored items, the sites would remain military bases, and UK security requirements would ensure that personnel had appropriate clearances. After discussions and negotiations (that lasted a year), we obtained a 'blanket' approval to allow the contract to proceed, though even today we are having to staff peripheral questions relating to who can drive vehicles, whether contractors can receive from stores or send to the stores and how FMS approvals can be extended to the stores companies without a third party transfer request now that they are contractor managed."[16]

Discussions with Canadian, Australian, and US contractors and officials demonstrated none of this was unique to the UK. While interviewees described numerous other examples, contractors (both in the United States and abroad) did not want to go public with them, fearing retaliation by US government personnel. Still, they repeatedly raised examples of maintenance and contractor issues that curtailed weapons availability for NTIB allies, in Afghanistan and elsewhere, as they waited for State Department licenses. Meanwhile, US contractors have become extremely risk averse, and constantly require the US government to clarify concerns, in order to cover any risk of triggering an ITAR violation and a potential fine. Of course, this slows down the process and has significant operational impacts; lawyers are pushing for full compliance while troops are put in harm's way. This should be completely unacceptable when it comes to nations fighting alongside the United States, but has become the norm.

An ITAR taint on a transferred product or system never goes away, and the issue of retransferring technology within the supply chain becomes a continuous headache for US allies—even for items one might consider not sufficiently important to be covered. This was highlighted in a case involving the UK's submarine force. The United States and the UK share the most sensitive information within a trusted community on nuclear and intelligence matters. However, this is not the case, for example, with nuts and bolts of US origin on military systems. In one case, a UK submarine refit was put at potential risk while it was at sea waiting on the State Department to approve a license, because some of the non-sensitive related components on the submarine were found to be ITAR controlled. As a result, this submarine could not dock and have its contractor service until the State Department approved it. The delay in obtaining retransfer approvals for these components risked delaying a maintenance program with a longstanding, trusted private contractor. Had that transpired, the UK's ability to maintain and operate one of its submarines could have been compromised. After significant diplomatic effort, State Department approvals were eventually received in time. One must question how long even a close ally like the UK will want to continue seeking the agreement of US officials to be able to maintain the ability to operate its key military capabilities.

One also has to question whether any of this is really a good use of scarce US resources. Is all of the excess bureaucracy really worth it? What is the United States getting out of this level of control? The NTIB governments, and the companies that work for them, need to go through significant bureaucratic hoops simply to enable the management of their own defense inventories. Many of these issues arise from the US government's requirement to give prior authority for the retransfer of US-origin items, even when these are not leaving the NTIB country, remain owned or used by the government in question, and/or are being managed on the government's behalf by cleared contractors. Yet, the potentially draconian legal consequences of risking an ITAR infringement have left many companies unwilling to risk undertaking work that they are cleared and ready to perform, without having State Department approval in writing. In these circumstances, ITAR retransfer provisions deny allies the ability to manage their inventories effectively, making their only impact on US national security negative.

However, the impact of ITAR taint is worse than just a concern over moving stuff around a supply chain. It is the biggest barrier to scientists and engineers working on joint collaboration efforts.

For example, using any US engineering assistance provided to a foreign person in the development of any new defense product means that product will be controlled by the ITAR, because the assistance provided by the US entity would be considered a defense service. This has huge real-world implications. Several firms

16 Information provided to author on a non-attribution basis.

whose members were interviewed had created policies to ensure that no US engineers could travel to or work in the UK (and vice versa), to prevent engineers from having conversations that could be construed as collaboration—and to prevent the knowledge so generated from becoming subject to ITAR, and no longer useful to these firms in the commercial marketplace. Companies now in the UK, Australia, and Canada are extremely careful about their cooperation with the United States, avoiding involving US persons in any R&D project. US companies with subsidiaries in NTIB countries do the same, and are aware that any discussions or cooperation can destroy shareholder value.

This "taint" includes a US citizen working abroad. An observer from one of the largest global defense contractors noted: "This US person could be living permanently in the UK and be a permanent employee of a UK defense company, for example, and according to...[the US government], everything he/she works on must be licensed from the US under a TAA...The US citizen is not exporting anything from the US and as he/she is not resident in the US or affiliated with any US company, how do they secure a TAA for the release of anything they may supply to their employer."[17] This is an impossible task, as one can hardly control what is in an engineer's head before he or she says it. Still, there is a requirement to upfront apply and get approval for a TAA to guard against that US person releasing US technology. Sources state that this same scenario has been raised numerous times with the State Department, and the only reply is: "They need a TAA." The only way this makes sense is if the US government's goal is not to have US citizens work in other countries. On balance, it does not make sense, and must be completely frustrating for foreign firms looking for direction. It is also a huge deterrent for foreign entities hiring anyone who holds US citizenship.

If the ITAR taint wasn't bad enough, the concept of extraterritorial application renders the control system even more onerous. Once an item has been exported, only the United States and Russia have a longstanding system of extraterritorial application of export controls in place to address retransfer of items or knowledge.[18] One should closely ponder why this is so. In practice, it keeps allies from selling their products, and also from moving their items from their home countries to the areas where they need to fight. For example, once an item, process, drawing, or piece of knowledge is labeled as ITAR, something truly remarkable happens—something that the United States has exploited for decades. Through an assertion of extraterritoriality rights to govern any retransfer of ITAR information, the United States essentially gains control not only of future sales of military equipment, but also of the military movements of its closest allies. This again happens because of maintenance. If a system with any US content breaks down in a country that was not a part of an original license, a new license is needed to get someone to repair it. This is the sword of Damocles lurking over the head of every system associated with the United States. This will lead to diminishing US export sales when countries get tired of going to Washington whenever they wish to deploy these systems or maintain them during deployment.

Extraterritoriality can also be triggered in other ways. One Canadian company was considering the possibility of establishing a repair-and-overhaul facility in the United States. However, this was quickly rejected by company leadership due to ITAR extraterritorial controls. For any item considered a defense item, repair and overhaul would be considered a "defense service" under the ITAR, and would place that item under ITAR control. This would then require a US export license to return the item to the owner, who—along with the country in which they were located—would be subject to the ITAR's reexport and retransfer requirements. Each time that item was retransferred or reexported, the owner would need to contact the US State Department for permission to move it.

The same concept of extraterritoriality is also impacting the use of test facilities located in the United States by its allies. Countries do not want to conduct defense-article testing, due to the defense services done on such articles placing them under ITAR control. Even Canadian companies are looking to Europe and beyond for this type of service, to avoid the US-origin controls—even with the higher costs of shipping these articles halfway around the world.

Unfortunately, interviews conducted in NTIB countries demonstrated that discussions on developing ITAR-free solutions have significantly advanced. This is in sharp contrast to the situation just a few years, when these types of plans were practically nonexistent in NTIB countries. The ITAR taint even applies to what most people would regard as *de minimis* levels of technology, and has prompted widespread efforts in many allied countries—but not previously in the NTIB

17 Email to author.

18 This may be changing. See next section. While US allies don't now have reexport controls, increasingly they will condition the export license on non-retransfer, which has the same effect.

countries—over the last several decades to develop ITAR-free products. These efforts have predominately started in continental Europe, and previously manifested themselves in the development of the European space and night-vision industries. In future, US firms and persons could become *persona non grata* when it comes to developing defense and commercial technology in foreign countries, and ITAR-free solutions will become the de facto way of doing business abroad. Foreign companies that include subsidiaries of US companies will increasingly find customers requesting proposals that contain no US-origin content.

The Barack Obama administration's Export Control Reform (ECR) Initiative moved many parts and components that were once controlled under the ITAR from the munitions list to the Commerce Department's EAR list. While these items should now be subject to *de minimis* calculations of the EAR, they were instead added to the new "600 series," informally called the Commerce Munitions List. During interviews, several companies and observers stated that the ITAR taint is still alive and well in the 600 series, and it appears that the United States has merely moved the overarching problem to another jurisdiction. The 600 series does not feature exceptions similar to those for technologies in the original EAR categories, which means more Commerce Department licenses need to be secured.

Extraterritoriality and the ITAR taint also encourage the dumbing down of technologies sold to the United States. Allies have been continuously burned when they have transferred technology to the United States—only to see that technology modified, made subject to ITAR, and not shared back. Foreign nations that provided the United States with technology to counter improvised explosive devices (IEDs) during the conflict in Iraq were particularly impacted in this way.

Overseas allies and defense firms (including US-owned firms) have learned from this. In discussions with senior managers, a leading strategy is now emerging, to develop two versions of systems and technology—one they keep for themselves and export to the rest of the world, and the dumbed-down version they give to the United States. The irony of the situation is the United States is now incentivizing less-capable solutions coming from abroad, but is buying them because even these products are better than what is currently being developed in the United States. This is similar to the US and US-export versions of the same technology that the United States had developed over the years, but now the tables are being turned. This is another example of how the ITAR prevents the United States from getting the best technology in the world. Cross-border cooperation would not only end this duplicate research, but result in superior products. This will not happen until the United States changes its export-control system criteria.

It would be bad enough if this two-product strategy only applied to overseas traditional defense companies, but the same incentives operate in the commercial world. The ITAR causes commercial firms to shy away from working with the DoD until after they commercialize their products, to ensure they can control and monetize their technology. Many dual-use firms have either been caught up in ITAR or seen others negatively impacted. The result is that more sophisticated firms have learned not to sell to the military first, to ensure that they can instead export their technology under Commerce Department rules. They have also learned to sell a dumbed-down version to the military under a different part number, or to conduct critical aspects of their R&D overseas, out of the hands of the ITAR. All of this undermines civil-military integration with Silicon Valley, which will be one of the most important relationships for national security in the future.

The US Chamber Commerce recently outlined many of these issues with the US export-control system, and how this ultimately hurts US industry and national security.

> "Many of the U.S. government's institutional arrangements and decision-making procedures for defense and aerospace export policy were established when American industry exercised far more control over global markets than it does today. A consequence of this economic and technical power was that the U.S. government was able to prevent or substantially delay the proliferation of a wide range of defense technologies by restricting American exports. Today, there are significant competitors in these markets challenging U.S. dominance of defense and aerospace exports. As a result, although their principal purposes include counter-proliferation and ensuring lawful use of defense articles, U.S. export restrictions now accelerate the establishment of more non-U.S. manufacturing and thereby indirectly promote the transfer abroad of defense industrial base capabilities.
>
> "This transfer is deleterious to vital American interests, including sustaining the technology, human talent and industrial capabilities necessary to maintain the United States military's advantages; sustaining and expanding American jobs; enabling political-military partnerships with foreign countries that reduce the burden on American soldiers deployed abroad; preventing the illegal use of

conventional weapons; and reducing the dangers of weapons of mass destruction (WMD)."[19]

The Threat of Reciprocity

Perhaps the United States will not change its export-control system until it is forced to do so. This leads to the question of what would happen if concepts of this system were applied to the United States? What if—in a world of globalized supply chains where most, if not all, US weapon systems contain some foreign content—US allies decided to or were forced to apply similar criteria for controlling their knowledge or technology (a reverse ITAR taint). What if they applied their own concept of extraterritoriality to this knowledge or technology, and made it retroactively apply to all US systems? It made sense when the United States and the Soviet Union applied an extraterritorial requirement on transfers and retransfers during the Cold War era, as these two countries dominated military technology for decades after World War II, and wanted to control the foreign policies of their client states. Changes in the technological balance of power could open the door for other nations to apply similar controls, as a means of trying to govern the actions of the United States.

One could hope that US allies would never want to adopt such a broken system, as they have seen firsthand the folly of such a technology-transfer system. Or, maybe they would avoid doing so out of self-interest, so as not to provoke the United States into doing all it can to eliminate foreign content; this might be the best argument for that decision. Still, if the likely US response to similar controls would be to spec out foreign content, then NATO allies moving to go ITAR-free in reaction to the US ITAR makes sense. It is entirely in their national interests to do so, but it should not be in the US national interest to encourage such a *fait accompli.*

The reality is that self-interest may not always be a consideration in motivating allies to change their export-control process to look more like the US system. One merely has to look at the United States, where the current export-control system clashes with self-interest, yet the country cannot make significant reforms. This scenario is no longer a far-fetched fantasy, as politics in allied countries may drive it. The German government's ban on the sale of weapons that include parts made in Germany may be the beginning of this trend.[20] In recent debate in the Canadian Parliament on Saudi Arabia's use of Canadian technology in Yemen, there were advocates lobbying for Canada to change its export-control system and apply the concept of extraterritoriality, exploiting possibilities for foreign policy control derived from the taint of domestic content.[21] So far, it seems the Canadian government will not act on this idea, but it is not out of the realm of possibility that future governments may be forced to do so. Any such reciprocity or mirroring of the US export-control system in these areas would cripple US operations, just as the "Mother May I's" to the US Department of State have negatively impacted allied operations.

The further erosion of US technological dominance will place the United States at risk of living under the system it has imposed on the rest of the world. The United States needs to access foreign technologies in the future. But, without harmonizing export-control regimes, it is quite possible that the United States will face the same types of restrictions that the UK, Canada, and Australia face daily in moving defense material around the globe. US military commanders would, rightly, not stand for such operational restrictions, but may have to get used to it if allies are forced to change their laws.

Before this issue progresses in allied countries, it is in the US interest to look at its own processes and assess the national security issues involved, including the risk that other countries' export-control systems could constrain US military operations in the future. At least in terms of the closest, most technologically advanced allies, the remnants of export controls are now primarily an outdated foreign policy lever—not a technological one—and changes could be made to ensure harmonization occurs. This would mean, for the United States' closest allies that have achieved levels of technological parity with it, eliminating the ITAR taint and the concept of extraterritoriality, and establishing a different transfer/retransfer regime. Still, there will always be bad actors within the United States and its allies. For that reason, this reform will need to take place within a trusted community of governments and companies. The NTIB is the perfect place to begin addressing these issues and harmonizing export controls.

For other countries, which have not achieved technological parity or established dominance in niche

19 "US Chamber of Commerce letter to Peter Navarro on Conventional Arms Transfer Policy," June 8, 2018," https://www.uschamber.com/sites/default/files/daec_cat_policy_submission_8_june_18.pdf.

20 "Berlin Strains Alliance with London as Saudi Arms Ban Frustrates BAE Deal," *Financial Times*, February 18, 2019.

21 See debate on Canadian bill C-47 (proposed changes to Canadian arms exports/permit regime). House of Commons Standing Committee on Foreign Affairs and International Development, https://www.ourcommons.ca/Committees/en/FAAE/StudyActivity?studyActivityId=9689599; Senate of Canada, https://sencanada.ca/en/committees/AEFA/Briefs/42-1?pageSize=50.

technologies, the current US export-control system may still be salvageable. Where the United States doesn't need the engineering talent or technology of these countries, the mechanisms of the ITAR taint and the extraterritorial application may provide some foreign policy value. Still, except for the latest technologies—for which countries may have no alternative to the United States—there will likely be constant erosion in the efficacy of export controls as a foreign policy tool as these nations go elsewhere for their defense needs.

Why Does the United States Even Need its Allies in the NTIB?

Some readers may ask, "So what?" So the system is inefficient and a burden on allies. Who cares if allies go off and develop their own technology? Besides, Silicon Valley is just a pain to work with and can't be trusted. Look at Google pulling out of the DoD cloud and AI efforts, while US private-sector firms set up R&D facilities in China that indirectly help China develop capabilities for the persistent surveillance of minorities and dissidents. How can these companies be trusted? The United States can just double down on the "Big 5" traditional defense contractors (Lockheed, Boeing, Raytheon, Northrop Grumman, and General Dynamics) and not worry about foreign or commercial companies. With all due respect to the Big 5, who can be incredibly innovative with the right incentives, this is not a sustainable strategy.

The net result of the US export-control system is that the country is missing out on emerging technology, and incentivizing a walling off of capabilities for which the United States needs to go it alone. That is already happening. If new controls on emerging technology do not directly discriminate against those the United States does not want its technology to go to (e.g., China and Russia), that will just incentivize that technology to move overseas. The Big 5 can't even maximize the talents of all their engineers within their own companies, because some of them happen to be based in Melbourne, Montreal, or Manchester. A looming question is whether the current US industrial approach is even possible anymore. The US defense-industrial base will not be able to remain dominant if it does not have access to global R&D, which will be increasingly choked off by barriers to the US market primarily created through the US export-control process.

The first argument for greater cooperation with US allies is there is only so much research and development going on in the world, and the trends have been moving away from DoD-centric research since the 1980s. In the aftermath of World War II, the US federal government dominated R&D spending. For example, in 1964, the federal government funded 67 percent of US R&D, and served as the leading spark for innovation in the US and global economies.[22] Today, the private sector, academia, and nonprofit organizations provide more than 88 percent of US R&D funding, with private industry funding almost 70 percent of the US total.[23] In addition, in the last several decades the forces of globalization have resulted in a declining US share of global R&D.[24] Just as the US government no longer dominates US R&D, US relative significance in global R&D is declining, in both the public and private sectors. In 2018, it was estimated that global R&D would equate to around $2.1 trillion dollars, with the US share at about 25 percent.[25] Based on the current government/industry split, US government R&D would equal about 3 percent of global R&D, while US private-sector R&D would amount to about 18 percent of global R&D, with academia and the nonprofit sector providing the remaining share.

This globalization and privatization of research and development is leading to a technological leveling on a global scale at the same time that new threats to the United States are beginning to emerge. Many of the technologies that will be necessary to meet and counter new threats are being led not in military labs, but in commercial ones. These technologies will be increasingly available on a global scale, to all who have the means to purchase them. If US national security agencies do not tap into the research, products, and business practices being developed in the increasingly globalized commercial sector, the United States will continue to lose the technological edge it has enjoyed since World War II, as potential adversaries incorporate these technologies and practices into their own military capabilities at a higher rate.

22 "Science and Engineering Indicators 2012," National Science Foundation, http://www.nsf.gov/statistics/seind12/c4/c4s1.htm.

23 Author calculations based on data contained in Industrial Research Institute and *R&D Magazine's* 2019 global R&D forecast.

24 The Defense Science Board found in 2012 that the globalization trend of the past several decades has seen a significant dispersion of R&D and changed the nature of private-sector R&D, as firms opened R&D facilities in China, India, Europe, Brazil, and around the globe, and that trend has only continued since then. Defense Science Board Study (2012).

25 "2018 Global R&D forecast," *R&D Magazine*, Winter 2018.

The winner in any defense-arms competition will be the side that can incorporate and blend military-unique and commercial technologies into new capabilities. The more companies working with the United States to try doing this will equate to more opportunities to field disruptive systems. An autarkic strategy based on five legacy monopolist firms, which increasingly do not compete with each other except at the beginning of a program before hardware is developed—combined with barriers to bringing in new technology—will relegate the US to technological inferiority.

Autarky and a "develop it all in America" approach will not work anymore. If the DoD and other US national security agencies choose not to take advantage of global commercial R&D and military R&D in allied nations, they put the United States at a severe disadvantage, as the government will need to replicate relevant global and commercial R&D. This costly developmental reinvention crowds out spending on more military-unique research. Absent open-acquisition policies and incentives for innovation sharing, the DoD risks allowing its potential adversaries to take advantage of a growing 97 percent of global R&D, while the US government attempts to leverage only a 3-percent share of global R&D, which is then further split between civilian and defense shares of government spending. The US government share of global R&D will continue to shrink, due to budget austerity and R&D spending increases in the rest of the world. In many areas, the United States still maintains a cumulative technological edge from decades of past defense-R&D expenditures, but there is limited private-sector R&D going into defense—and what is there is mostly subsidized through government contracts and R&D reimbursements.

One can hope that China will ultimately adopt the centralized model that relies on state-run, defense-dedicated R&D within China, rather than the open, civil-military integrated model. In the long run, even if that unlikely outcome were to happen, it is questionable that the same US defense-industrial-base model that won the Cold War against a competitor with an equivalent population and a state-sponsored R&D industrial model can compete against an adversary four times as large doing the same. The United States still has the current advantage when competing with China, but that advantage is rapidly eroding. In the future, it may well be found in several numbers: population, number of scientists and engineers, and gross domestic product (GDP). At this aggregate level, the United States will need to increase these numbers to out-innovate and compete; the only realistic way to do that is to have more allies integrated into the US defense economy.

Right now, the two economies are moving toward parity in terms of GDP, with the World Bank saying China's economy on a purchasing-power-parity basis has already overtaken the United States.[26] Overarching GDP is the pool from which defense spending can be excised. If a country four times the size of the United States continues to grow, and ultimately achieves per-capita GDP equivalence—and proportionally maintains four times the number of qualitatively equivalent scientists and engineers available to undertake R&D—the United States will never be able to catch up. In this scenario, the United States will be like the Soviet Union, and eventually break its economy trying to compete militarily with China. Obviously, greater R&D productivity, based on a higher quality of the science, technology, engineering, and math (STEM) workforce, is one way to compete, but can the United States be four times as productive per R&D expenditure? Otherwise, it will need to look to expand the population, the economy, and the STEM workforce base. Realistically, that will not be done through organic growth or immigration, but could be done through leveraging alliances and STEM cooperation, and also by improving productivity through leveraging global commercial R&D.

Things look better against Russia. If one looks at a straight comparison between the United States and the Russia of today (which lost its population parity with the United States after the breakup of the Soviet Union), the United States is almost twice as populous, and will likely have a greater number of engineers and scientists to compete against Russian aspirations. Still, the Russians have been able to overcome their economic and population disadvantage by focusing their R&D expenditures on disruptive technologies, and by taking advantage of technology globalization to outmaneuver the United States.

The next point to consider is the success of the US strategy to go it alone during the Cold War. Under a historical lens, this standalone approach with regard to technological superiority may well have rested on a myth. It was not only US scientists and engineers who won World War II and developed the Cold War systems through the 1970s. United States technological advantage began with a massive transfer of technology from the great power of the time—the United Kingdom—through the Tizard mission, and then through continued cooperation during World War II. It also must be remembered that the United States was

26 "World Development Indicators Database," World Bank, January 25, 2019.

able to leverage European scientific and engineering talent that crossed the ocean, both prior to the beginning of World War II and after the war. Even German scientists who served the Nazis, such as Werner Von Braun, were instrumental to US missile programs once they moved to the United States. These scientists and engineers served as the backbone of the great-power competition with the Soviet Union in the 1950s and 1960s, and during the second-offset advances in the 1970s. The United States has always relied on foreign scientists and engineers in the defense-industrial base, but seems to have conveniently forgotten much of that history, as it has placed barriers to accessing those scientist and engineers in the last four decades.

Following its victory in the Cold War—just as the generation of World War II scientists began to die out—the United States took a holiday from defense development and procurement. Technological leadership transferred to the commercial market, which also relied heavily on immigrant scientists and engineers creating the startup culture known today as Silicon Valley. The past US comparative advantage in innovating, both militarily and commercially, has been the ability to attract the best and the brightest from around the globe. The other innovation lesson to be learned is the push and pull of civil-military integration of the industrial base. Innovation is now being driven in the commercial market, but the roots of this innovation are military. With the essential civil-military integration in the United States after World War II, it should come as no surprise that the genesis of the commercial US electronics and computing industries took place in the Route 128 Corridor in Massachusetts and near Stanford University in California—areas that were once hubs of military electronics and radar development, prior to the creation of the integrated circuit.

So, how can the United States compete with China in the future? First it will take population. The population of the Western Alliance—the United States, NATO, and the European Union (EU), plus non-NATO allies such as Japan, South Korea, Australia, and Israel—stands at about 1.2 billion, which is close to population parity with China. It is currently four times the economic capacity of China, as measured by GDP. The current reality is this "Western Alliance" is a paper tiger, extremely inefficient in its technology development, as—given current tech-transfer and cultural barriers—there are few mechanisms to get those 1.2 billion people to cooperate on industrial development in any meaningful way. Duplicative developmental reinvention occurs throughout the alliance.

A first step to recreate and energize such an alliance is to establish the right culture and processes within the NTIB. The NTIB countries would add the capabilities of 128 million people to the United States' 326 million, or a gain of about 40-percent capacity. While this grouping is not going to be able to compete with China in the long term, it can help in the short term by doing something even more important. The NTIB can be the bridge or mechanism to experiment and figure out how to leverage industrial cooperation with the United States' closest allies to compete in the middle part of the twenty-first century. The United States will eventually need an industrial base larger than just a combined US/UK/Australia/Canada entity, but it needs to start somewhere. If the United States can't establish the right mechanisms for cooperation with these countries, which have so many shared historical and cultural ties, it is doubtful it will be able to do so with anyone else.

The NTIB countries start with many advantages. They already share most US values, are working on the technologies the United States needs in the future, and have a history of more than a century of cooperation. These countries' engineers speak the same language and, in many cases, work with companies that exist in all four countries. There already exists within the NTIB a culture of cooperation on intelligence (with the "Five Eyes" alliance), on operations around the world, and on nuclear issues. The sensitivity of the information being transferred between the NTIB countries in intelligence and nuclear matters far exceeds what is needed under defense-industrial-base cooperation. It makes no sense to have greater controls on less sensitive matters within the NTIB, but that is the situation today.

Further Observations on the NTIB Industrial Base (United States, UK, Canada, and Australia)

The September 2018 executive-branch study on the US industrial base was significant, but not surprising.[27] That study outlines the toll of the post-Cold War downsizing of the industrial base. Eventually, tens of billions of dollars will be needed to address shortfalls in military-unique manufacturing and industrial capabilities, to support a ramp up in production of munitions and large weapons platforms. Innovation has been crowded out of the system, and competition has declined due to the consolidation of the US defense industry. This first occurred at the prime-contractor level, but has increasingly been felt as the middle tier has been hollowed out

27 "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States."

through further consolidation, buyouts, and the lack of new programs. The small-business sector is not as healthy as it once was, as the number of new-entrant firms has declined, as has their survival rate.[28] Whether "graduation" is defined as becoming a larger contractor or moving on to the commercial sector, very little graduation has happened. In fact, small businesses working for the federal government face an increasingly impermeable wall as they are being trained in a compliance-based government contracting system that is not conducive to working in the commercial market.

The problem the United States faces in competing in scale against a potential aggressor like China will not only be found in manufacturing, but also in innovation. For the moment, China has won the manufacturing battle. The United States needs to claw back this capability and source from more secure supply chains, but China has yet to win the competition for ideas. Unfortunately, many of these ideas will be found in startups starved for cash, engineers looking to set off on their own, nontraditional firms, and overseas entities. The DoD needs to tap into this innovation before the Chinese do. The United States has put up huge barriers and disincentives to working with this culture of innovation. The Chinese have not done so, and have been actively courting these startups with venture capital, in Silicon Valley and around the globe.

The NTIB offers the opportunity to immediately add 40 percent in capacity to the US industrial base. If done right, this can provide additional scale and fill some of the manufacturing holes that currently exist. Most importantly, the UK, Canada, and Australia have not yet created the types of disincentives for the commercial industrial base to work on defense matters that the US has created. This offers them a significant comparative advantage to the United States when trying to tap into the more innovative solutions now coming out of that industrial base. Each country has its industrial weaknesses, but also maintains a series of defense-unique specialties and a growing commercial base to work with its military-unique base. It will be important for the United States to leverage these capabilities.

Observations on the UK Industrial Base

The UK is the largest of the non-US NTIB countries. Sixty-six million people support a defense budget of £48.3 billion, or around $62 billion. The industry group representing the aerospace and defense sector in the UK has more than one thousand members; more than nine hundred and fifty are small businesses. The UK's military-unique sector still comes close to supporting standalone industrial capabilities in shipbuilding, air, ground, space, and missile systems, with annual sales of £23 billion and £5.9 billion in UK exports (2016 numbers). Large UK companies—such as BAE, Rolls Royce, Ultra, Meggitt, and Qinetiq—have significant US subsidiaries that operate under special security arrangements. For the most part, all large US defense firms have facilities and operations in the UK.

It seems that current US export-control processes disproportionately affect the UK; unfortunately, that is a result of being the United States' closest ally. Through the breadth of its bilateral activity with the US, the level of defense trade between the two countries, and its increased use of outsourcing within its industrial supply chain, the UK is the country most punished by the US export-control system. According to UK officials, there has been more than a four-fold increase in the number of retransfer requests they have had to submit in the last four years. The Defense Trade Treaty with the UK, which was designed to alleviate some of this burden, has been a complete failure, as it has not lessened any of the bureaucratic hurdles. Discussions within both Canada and Australia revealed many of the same issues with regards to ITAR and technology transfer. Through its ITAR waiver, Canada obtains some relief for a number of routine transactions, but, surprisingly, not a lot for anything else that would encourage close collaboration. The main difference is there are more routine transactions in the UK, and the US bureaucracy cannot keep up with the situation. As a result, the timing of reviews and approvals becomes problematic, translating into periodic crises when licenses aren't approved quickly.

The US-UK technology-transfer relationship during the latter half of the Cold War was primarily a one-way street. US technology went to the UK, with a stringent US control structure put in place. In those cases where the UK had more advanced technology (for example, the use of counter-IED technology developed in during the conflict in Northern Ireland), this technology was transferred to the US government with no strings attached. This act of being a good ally was subsequently not rewarded, as any improvements made in the United States were not shared with the UK. This relationship

28 Samantha Cohen, Gregory Sanders, and Andrew Philip Hunter, "New Entrants and Small Business Graduation in the Market for Federal Contracts," Center for Strategic and International Studies, November 20, 2018, https://www.csis.org/analysis/new-entrants-and-small-business-graduation-market-federal-contracts.

between a dominant partner and a secondary, lesser source of technology is still in place—even though the UK has the potential to develop technologies similar to, or even more advanced than, those of the United States.

This legacy control system will keep the relationship from evolving in the future, and the barriers put in place will ensure that the United States and the UK will continue on a path of developmental reinvention. This is important because the UK has developed a series of military niche technologies that would reduce the R&D time necessary for US companies to replicate them. More importantly, there are areas in the UK economy in which commercial advancements being made in dual-use areas—such as financial technology, the oil and gas industry, and commercial space technology—that can be applied in the military sphere. For example, the data analytics and algorithms necessary to analyze large data sets in the financial sector are easily applicable in the machine-learning applications that the Department of Defense will need in the future. The UK oil and gas industry has been developing a focus on underwater autonomous vehicles, as well as underwater technologies that will be applicable to anti-submarine warfare and other undersea operations. Finally, the commercial space sector developing in the UK will have significant military operational potential.

The most troubling observation about the US-UK relationship is that Brexit is now compounding the changes being brought about by the history of failed attempts to bring the two industrial bases together. The failure of the 2008 US-UK Defense Cooperation Treaty has put a damper on the expectations of the NTIB within the UK industry. Many do not believe that the US bureaucracy will allow much progress to be made through the NTIB.

Brexit is now forcing a reevaluation of the UK's role in the world. Unless the United States embraces greater cooperation with the UK, it is probable that the UK industry and government will begin to focus more on developing ITAR-free military applications. Even more interesting is the thought process that may move the UK to cooperate more with non-European and non-US companies, such as those in Japan, Israel, India, South Korea, and Turkey. The NTIB cooperative project probably has about two to three years to show real results before the US technology base is essentially limited in its upside cooperation with the UK. Cooperation will likely still continue, but will be limited to being more legacy and backward looking, rather than focused on forward-looking technologies and applications.

Unlike discussions with UK defense participants in the last two decades, recent conversations as part of this study revealed the desire of actors in the UK to develop ITAR-free technology. In the absence of reform, the likely result is the end of the one-way street of technological innovation from the UK. The United States will get a second version, or tier, of technologies from the UK (as is already the case from its other allies), while top-tier technologies will be developed through partnerships with other countries and not shared with the United States. Given the current security and export-control relationship, and the history of the UK being shut out of the benefits of its technology sharing, there is a serious lack of desire to ever again bring in the crown jewels to the United States. The view that technology has been a one-sided affair, in which the United States takes all the best technology of its allies but does not reciprocate, will lead to a future in which the United States will not be able to take advantage of what is being developed in the global marketplace. This will happen with both military-unique and commercially derived technologies. The United States is increasingly seen as a poor customer and ally, and that will eventually have a cost, even with its closest allies.

Observations on the Canadian Industrial Base

With thirty-seven million people, Canada has a population on par with that of California. Since World War II and the Hyde Park Agreement, Canada's defense-industrial base has historically been the most integrated with the United States'. Canada created one of the world's strongest defense and aerospace industries during World War II, and truly became the arsenal of the British Empire—particularly before the United States entered the war. This capability significantly degraded over the years, and went into freefall at the conclusion of the Cold War. Still, there is a strong legacy defense-industrial base, and a much stronger dual-use base that primarily focuses on the civilian market.

Canada currently spends about $25 billion Canadian, or about US$19 billion, on defense, which is about 1.3 percent of GDP. Canada may have a counting problem, as it actually spends more than that on national security needs in other parts of its budget, which are counted in other nations' defense-budget baselines.[29] Still, even with those expenditures added in, Canada is still far below the NATO goal of spending 2 percent

29 NATO countries account for defense spending in different ways. While some countries include expenses for cyber defense, the national police or gendarmerie, border security, coast guard, as well as healthcare costs for troops and veterans, Canada does not include any

of GDP on defense. This is of current concern, as the Canadian government has no plans to ever meet the 2-percent threshold that the current US administration holds as a benchmark. This could hurt potential expansion of defense cooperative efforts if the US administration decides to act transnationally, rather than in its broader interest. The US action of imposing steel tariffs on Canada falls into this category, and future progress on solving these types of trade issues will probably not be helped by low Canadian defense spending.

The Canadians are planning to step up investment in the modernization of the North American Aerospace Defense Command, including renewal of the North Warning System, and have committed to increasing defense spending by 70 percent between 2016 and 2026. The jury is still out as to whether these plans will actually be executed.[30] Despite growing threats to Canada's territorial sovereignty in the Artic, it remains to be seen whether the Canadians have the ability or will to spend more on national defense. Despite legacy historical ties, this could translate into Canada being the weaker partner in any defense-specific NTIB until it increases defense spending.

Still, the Canadians have a strong ground-vehicle sector, anchored by General Dynamics Canada, which is highly integrated with the US ground-vehicle industrial base. Exports, particularly to the United States, are extremely important to maintaining current Canadian defense-industrial capabilities. While most Canadian defense firms would be considered small businesses in the United States, significant innovation exists in those companies. For example, smaller niche companies in maritime-domain awareness and optics will continue to serve as sources of defense-technology advancements. Also, significant national capability exists in the dual-use aerospace firms—such as CAE in aerospace simulation and MacDonald Dettwiler and Associates (now a part of US-based Maxar Technologies) in space—that have needed to focus on export and commercial markets to maintain their competitive edge. The most compelling future contribution Canada may make to allied defense may reside in the commercial information-technology industry based in Waterloo, but also increasingly in Vancouver, which is becoming more integrated with the Seattle/Silicon Valley innovation clusters.[31] Advances in cybersecurity and quantum computing are beginning to emanate from these innovation hubs.

Observations on the Australian Industrial Base

Australia comprises almost twenty-five million people, a number comparable to the population of Texas. Despite a population much smaller than Canada's, Australia far exceeds Canadian defense spending, currently spending around $35 billion Australian, or about US$25 billion. The Australian industrial base is not as robust as the industrial base in the UK. It primarily depends upon US and European prime contractors who perform a majority of work in their home countries, and are then supported by a smaller, niche-level Australian defense-industrial base that serves as subcontractors to the overseas primes. This seems to be changing, as the Australians are interested in strengthening their indigenous defense-industrial base.

That is not to say that the Australian defense-industrial base is not innovative, or could not serve as the nucleus of a much stronger industrial base. In one area, the Australian industrial base is on par with, or has even leapfrogged, the United States. New advances in future radar technologies were developed indigenously by a small Australian company that, despite the odds, was able to pursue rapid development in a way that was not incentivized in the United States. Despite a technology that is potentially a force enabler in the United States, and a large investment by a US prime, there are significant barriers to bringing this technology to the United States—not least of all, dealing with future ITAR implications. Progress has been made, however, in using this technology as a test asset, but real collaborative work will likely need to wait on future reforms.

This experience is another reminder of the defense-industrial base's potential to be disrupted by a small number of scientists and engineers in the equivalent of David Packard's garage. There is huge potential for a Silicon Valley-like experience to be replicated not just in the United States, but also in its closest allies, through the right incentives. In this and other technology niches, the Australians continue to provide examples of how small-business innovation can potentially disrupt the defense industry, just as small startups have continuously disrupted the commercial information-technology industry during the last three decades.

Australia also has several national security and commercially derived technologies that, with a greater

of these in its defense budget, which is used as a benchmark to meet the 2% NATO spending goal.

30 Ken Hanson, "What's Happening to Canada's Defence Spending?—Despite a Policy Overhaul, the 2018 Budget has Set Out Virtually No New Spending for the Fundamentals of Canada's Military. That's a Problem," *McLean's*, March 6, 2018.

31 For background on Canadian advances in quantum computer, see "Canada's Quantum Valley: An Integrated Pathway to the High-Tech Future," Hudson Institute, October 16, 2018.

effort, could be applied to the defense realm. There are ongoing Australian efforts exploring the possibilities of quantum radars. The breakthrough in autonomous operations by the Australian mining industry, which conducts robotic operations in overseas mines from command centers in Australia, could have significant potential military applications. Substantial Australian research is being conducted in quantum computing, and in the medical and biotechnology fields. While the private-equity/venture-capital infrastructure is weaker in Australia, the venture-capital community based in Silicon Valley is well aware of these advancements, and is providing capital to pursue future opportunities.

Like the UK, Australia is increasingly stymied by the ITAR. And, like other US allies, it is pursuing strategies to protect its best technologies and keep them away from the US ITAR system. The Australians also have some important assets that could be used for future dual-use and military testing. The test ranges and air and sea space around Australia can serve as a test bed for future aerospace hypersonic- and autonomous-vehicle development. Current ITAR rules will encourage Europe, Canada, Japan, and others to use these test facilities in Australia rather than testing their prototypes in the United States, or cooperating with the United States on these projects.

Parts of Australia seem to be waking up to impending threats from China, but the politics may not have caught up yet. It remains to be seen whether any future change in government will have national security implications. Another future risk manifests itself in how Australia conducts research. A huge amount of its R&D in performed in its universities, but the financing of those universities depends to a great degree on foreign, mostly Chinese students. While this same dynamic exists in the US, UK, and Canada to a certain degree, and could be a topic of discussion in the NTIB, the scale of defense R&D open to Chinese espionage may be greater in Australia, based on the level and quality of R&D funding directed toward the university system there.

Barriers to NTIB Collaboration and Cooperation

Barriers to NTIB collaboration primarily fall into two areas: process and culture.[32] Process barriers include the acquisition and export-control processes, but also the idiosyncratic management processes that have developed in all four countries. The US acquisition process is a huge barrier for nontraditional US firms to break into and work with the DoD, let alone the additional constraints faced by a foreign firm. On the export-control compliance front, foreign companies in the NTIB must face not only compliance with their own countries' export-control system, but at least five different US technology-transfer regimes, depending on where they are based—and many of these companies are based in all four NTIB countries. There are the ITAR, the Commerce Department's dual-use system, the Canada ITAR waiver for unclassified-goods control, the Australia-UK Defense Trade Treaties, the Foreign Military Sales program, and any terms associated with cooperative R&D agreements. Making sense of all of this requires a compliance army of lawyers and clerks, burning up a significant amount of resources. The cost of this compliance is greater than just these direct costs, and is felt more through disincentives to innovation and loss of worker productivity waiting for approvals before work can be started.

The second level of barriers is cultural. While the acquisition and technology-transfer process barriers are important, it is primarily culture that keeps the United States from addressing them, so culture is really the most important issue. In the United States, it can be argued, that culture primarily derives from victory in the Cold War. The United States has become hamstrung by learning the wrong lessons from this conflict. US management processes suffer from a belief that these processes delivered a victory against the Soviet Union and, thus, that there is no reason to change them. Technological dominance came from centrally managed, government-sponsored programs during the Cold War, and a culture of autarky rests on this success. The lack of trust in US allies and the commercial market has its foundation in this belief that centralized planning and autarky won the Cold War.

Only a reevaluation of the Cold War mindset will lead to any culture change, as the maintenance of current US policies is embedded in this belief. While stuck in a Cold War culture, policies will continually manifest as processes grounded in autarky. The United States needs to first admit that the world has changed, and that the threat environment and competitors are different than what they were in the Cold War. Then, it must

32 "National Technology and Industrial Base Integration: How to Overcome Barriers and Capitalize on Cooperation," Center for Strategic and International Studies, March 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180307_McCormick_NationalTechnologyAndIndustrialBaseIntegration_Web.pdf?Yd28kTbbpfedujBec.QYCbUtwMDC4qaJ.

recognize that the US military has lost, or is losing, its technological edge. No serious change in mindset can happen until those two realities sink in.

Leadership is needed to try making the necessary changes, which transcend defense cooperation with allies, but the current bureaucracy seems impervious to change. The key is for the national security consensus to change, and for leadership to be provided by civil servants and political leaders who can pull together strategy, budgets, and process reforms as a way to incentivize industry to provide the necessary solutions to meet emerging great-power threats. Congress has a significant role to play, and a bipartisan majority of the members on the national security committees will need to understand the new environment, in order to provide cover for the executive branch and the bureaucracy to embrace this change.

Still, a newfound majority consensus and recognition of what is in the US national security interest won't necessarily allow for opening the aperture on cooperation and export-control reform. First of all, consensus is hard to obtain; there will be many who do not accept that China may be a threat, or that the United States is becoming technologically inferior. There will be many who will not accept that foreigners or commercial firms have anything of value that the DoD needs, let alone that they are holding back from selling to the US government. It will be hard to overcome the belief that companies will always sell to the DoD, either out of patriotism or greed from making profits on government contracts. The problem is that while greed may be a factor, the commercial and Chinese markets now offer greater profits than the DoD market. Allied governments and private-sector firms may want to help the DoD, but it is no longer in their economic interest to do so. It is up to the US government to figure out how to shift that equation.

The other issue is that some in Congress, and elsewhere in the US government, like the leverage that the export-control process gives them over industry and the foreign policies of other nations. This tool has been wielded for decades and, even as the system's negative consequences for innovation and the technological balance of power begin to reveal themselves, it will be extremely difficult to convince those who wield this power to give it up.

Those who exercise this power and undercut US innovation maintain a perception that US allies cannot be trusted. This trust has been undermined through a status-quo playbook that highlights examples whenever an ITAR violation has occurred, no matter the significance. Examples of "wrongs" done decades ago are still being used to question the ability to trust Canada, the UK, and Australia, even though these countries are trusted with much more sensitive data in other areas. This also ignores the fact that the basis for most technological leakage over the last several decades has always existed in the United States, as demonstrated by the number of Justice Department cases of espionage and technology-transfer violations, as well as US ITAR violations that have come to light. NTIB allies have been too diplomatic to point out these cases.

Unfortunately, the publicly unstated but privately shared view—revealed during interviews with many US allies, and not just those within the NTIB—is that these nations do not trust the United States to control technology within its own borders. It is, by design, a massive defense free-trade area within the fifty states. Adversaries have taken advantage of this to steal much of what the United States unleashed the ITAR bureaucracy to keep them from obtaining. This leakage was achieved through classic espionage techniques, but also because US firms and persons were able, at the bequest of adversaries, to illegally smuggle technology out of the United States. US security may have a fatal flaw in its trust of its own citizens, some of whom may be less trustworthy than foreigners—especially those with a reciprocally recognized security clearance. While Customs and the Department of Justice stepped up enforcement of actual physical goods illegally leaving the United States, the action quickly shifted as the reality of today's cyber world set in. It is now easier to just steal what is needed from the United States from the confines of Shanghai or Yekaterinburg, rather than establish an entity to do so in the United States—although such an entity can still be a source of data collection and poor cyber hygiene, allowing "friendly" hackers to steal from it.

This trend has been noted in discussions during this study, with several views expressed that the United States is no longer considered a reliable partner to protect foreign technology. This is seen through its unreliable information-security regimes, government labs and acquisition officials who do not respect the intellectual property (IP) of allied countries, and finally the aforementioned issue of ITAR taint, as foreign technology becomes wrapped up in US export constraints as if the United States had originally developed the technology.

The US government needs to look inward for a moment, to ponder how adversaries were able to steal US technology, and the how US innovation machine is being constrained by the way the government protects

technology. Technology theft did not come about because US friends and allies didn't follow the law; instead, the United States worried about others while leaving the door to its own house open. Now, the law creates disincentives to innovation with allies, to protect information that has long been transferred to enemies that will never follow US laws.

Additional barriers and threats to the NTIB are emerging. The rise of protectionism in the United States could be damaging, if it does not discriminate between allies and potential enemies. Frustrations with burden sharing, and the willingness of future governments throughout the NTIB to spend what is necessary for defense, will create frictions. Still, the biggest threat is whether US allies and Silicon Valley just throw in the towel rather than wait for the United States to make the changes necessary to further cooperation. This could be triggered by changes in government, or by the US government being seen as incapable of change or of protecting other countries' technology and IP. Without the United States changing policy to address new and compelling threats, and a recognition that US technology dominance is fading, current NTIB efforts may only result in a cursory nod to the new law. The United States would continue ignoring the industrial capabilities of its closest allies and the underlying globalized commercial-industrial base, and they would be forced to reciprocate.

Post-Brexit, the UK will need to navigate a different set of assumptions and policies regarding what is in its national interest, and other allies face similar choices. ITAR-free solutions for military goods may become the norm, and new industrial partnerships may form. Developmental reinvention would happen on a grander scale. Silicon Valley can play regulatory arbitrage as to where to conduct business and R&D. Much of this will be done quietly, under the surface, and will not be broadcast to the US national security community. De facto changes will happen in boardrooms and briefing rooms around the world, on a policy and transactional basis. The net result is the best technology will not be offered to the United States—and thus will no longer be available when needed. Perhaps the most significant finding of this study is not that the United States is losing, or has lost, its technological dominance, but that many foreign and domestic firms do not want to share with the US government—or at least not share their best technology—and this problem is likely to get worse without further US action.

Status of NTIB Implementation

US industrial-base relationships with Canada, the UK, and Australia have undergone significant evolution since the end of the Cold War. The NTIB with Canada was established in 1994; however, the ITAR waiver for Canada—which recognized the interconnectedness of the US and Canadian industrial bases—was already established when the ITAR was established in 1975. It carried over a longstanding export-license-free zone established at the time of the Hyde Park Declaration of 1941. The end of the Cold War put great pressures on US-Canadian cooperation, as companies merged and went out of business, and the industrial base on both sides of the border atrophied—moreso on the Canadian side, as defense expenditures plummeted and Canada, like the rest of the United States' NATO allies, reaped its "peace dividends."

In 1999, the United States had an epiphany of sorts during the Loral and Hughes cases of tech transfer of missile technology to the Chinese.[33] Subsequently, export-control policies were tightened on space and missile technology, and established for other exports and knowledge. In retrospect, this tightening should have been targeted specifically to China. But, because they were designed to be nondiscriminatory, these policy changes unleashed all sorts of unintended consequences. The first manifestations of these new controls were the rise of the European ITAR-free space and night-vision industries. Also, at about this same time, it came to light that Iranian front companies were taking advantage of the Canadian ITAR exemption to move defense and aerospace spare parts to Iran. This resulted in the United States overreacting and weakening the Canadian ITAR exemption.

Some good did come out of this, as the Canadians established a controlled-goods program for unclassified dual-use items covered under the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies and US ITAR items.[34] This system, based on a trusted set of companies, was successful in gaining control of the internal transfer of goods within Canada. The United States did nothing of the sort, and was too trusting of its own citizens and law enforcement to control inter-US transfers. Adversaries took advantage of that flaw. Technology has been illegally flowing out of the United States as the focus of potential adversaries

33 For a history of these transfers, see "Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China," May 25, 1999, https://www.govinfo.gov/content/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851-1-2.pdf.

34 Forty-two countries currently participate in the Wassenaar Arrangement.

switched to cyber espionage and establishing front companies in the United States. Meanwhile, the United States was successful in keeping that technology from moving freely to countries that play by the rules. So, while the United States believed the threat was with its allies and required more stringent export controls on items that had legally left the country, lax controls elsewhere in the US supply chain provided opportunities for China and Russia to pick its pocket through espionage and cyber theft.

After 9/11, several allies rose to the occasion and transferred technology to the United States, with no strings attached, to help in the Afghanistan and Iraq conflicts. In particular, the UK transferred the counter-IED technology and knowledge learned in the conflict in Northern Ireland. The United States repaid this altruistic transfer by applying the ITAR taint, and prohibited any counter-IED technology from going back to allies without a license approved by the State Department. The conflicts in Iraq and Afghanistan further illustrated some of the greater problems with the ITAR, which continued to put up barriers to the US fighting side by side with its allies, and created miles of red tape to do so. Perhaps most importantly, it illustrated how low the United States had fallen from the ability to apply common sense to its foreign and military relations—wrapping itself up in bureaucracy to control a nut or a bolt that had been triggered by the application of the ITAR taint and extraterritoriality applications. While most, if not all, licenses to allies were eventually approved, they all created unnecessary crises and time delays, for no purpose except to increasingly drive wedges between the United States and its allies.

It was to overcome some of these technology-transfer barriers that the George W. Bush administration unsuccessfully tried to persuade Congress to provide for legal changes to exempt the UK and Australia from certain export-control applications, and then initiated separate treaties in the mid-2000s. The history of the treaty negotiations and ratifications was fraught, with antibodies in the administration and Congress bent on destroying the project. Looking back, one can conclude that they succeeded. These forces did not want to see any changes to the Cold War export-control process and, to their credit, truly believed they were acting to protect national security. While ten years ago, the impact of their views was probably only process and operational inefficiencies, in today's environment these views are certainly applauded in Beijing and Moscow, as the net result will be increasing US technological inferiority.

The Defense Trade Cooperation Treaties were signed in 2007, and ultimately ratified in 2012. It was questionable whether the treaty route or changes to Title 22 of the US Code were the most advantageous, as the US administration likely already had the authority to offer the same Canadian ITAR exemption to the UK and Australia but chose not to, out of fear that Congress would overrule it.[35] Regardless, these treaties were failures. As one participant in the treaty negotiations stated, the treaty "was intended to provide a comprehensive framework for Exports and Transfers, without a license or other written authorization, of Defense Articles' between our two countries. That ambition has not yet been realized. The Treaty implementing arrangements are insufficiently attractive for companies to use them."[36]

With the failure of the UK and Australian treaties, and the limitations made to the Canadian ITAR exemption, tangible research collaboration and industrial integration between the United States' closest allies was difficult, if not impossible, to implement. Some in Congress believed a new approach was needed to meet new threats in an era of technological diffusion and an emerging great-power competition. A different regime was required for the United States to better leverage the technological possibilities that exist not only in allied military-defense industries, but also in emerging technologies that reside in the globalized commercial industry, within both the United States and its closest allies. It was to achieve these goals that, in 2015, Congress—led by former Senate Armed Services Chairman Senator John McCain—began reforms to remove bureaucratic barriers to rapidly accessing the technological advancements residing in the commercial and global defense industries.

As part of these reforms, Senator McCain decided to leverage an old concept—the NTIB. The senator proposed adding the United Kingdom and Australia to the definition of the national technology-industrial base in section 881 of the 2017 National Defense Authorization

35 For a different perspective, see "U.S. Weapons Technology At Risk: The State Department's Proposal To Relax Arms Export Controls to Other Countries" (report of the Committee on International Relations of the United States House of Representatives), May 1, 2004, https://fas.org/asmp/campaigns/control/US_Weapons_Technology_At_Risk.html. In retrospect, the administration at the time may have been able to use its own regulatory powers to address these barriers, but was deterred from doing so by the concern that the Foreign Relations Committees would tighten the law and prohibit such an approach. Thus, the treaty path was taken, and the option for regulatory action was maintained for a future time when the political dynamics in Congress had changed.

36 Email to author.

Act, and Congress subsequently did so. Congress intended that these four countries embark on closer industrial-cooperation and technological-cooperation efforts, to achieve breakthroughs in defense capabilities.

As part of the 2017 NDAA, the secretary of defense was required to develop a plan by February 2018 to reduce the barriers to seamless integration between the persons and organizations that comprise the national technology and industrial base. The DoD NTIB implementation plan required by the 2017 NDAA was included in the annual industrial capabilities report that was published in March 2018. Subsequent reporting on NTIB progress is required, by law, to be included in each of these annual reports. The March report outlined the following four NTIB pathfinder efforts.

> "• **NTIB Governance:** A foundational project to formalize governance among the NTIB nations. This pathfinder project includes a nonbinding Statement of Principles among the NTIB countries, appointment of national representatives by the NTIB partner nations, and the creation of an NTIB International Staff Working Group to address any outstanding issues.
>
> **"• Investment Security:** Pathfinder on development of a potential consultation mechanism to better share information between NTIB countries regarding foreign direct investment (FDI).
>
> **"• NTIB Controlled-Technology Transfer:** Pathfinder to review possible models for facilitating controlled technology transfer, including the Canadian controlled-goods program.
>
> **"• Cybersecurity for Small-to-Medium Enterprises:** Pathfinder that will explore barriers to and opportunities for improving cybersecurity in small to medium enterprises within the NTIB in a cost-effective manner, such as using cloud-based solutions and compliance with NIST 800-171, Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations."[37]

The NTIB implementation report was then in a sense overshadowed by the industrial base study established by Executive Order (EO) 13806, as further NTIB analysis folded into the larger defense-industrial-base effort. Still, during this time, the NTIB countries met and worked on the NTIB pathways projects. The EO 13806 study, completed in September 2018, endorsed greater integration within the NTIB through a recommendation to work "with allies and partners on joint industrial base challenges through the National Technology Industrial Base and similar structures."[38]

NTIB countries have modified the original pathfinder projects, and are currently working on four "lines of effort" that focus activities on: cross-cutting enablers; industrial-base protection; small- and medium-enterprise (SME) integration; and human-capital development. It appears the most significant progress made so far has been on plans to harmonize foreign-direct-investment strategies, to protect emerging technologies from being stolen by foreign actors. The NTIB countries met again in March 2019 in Australia to discuss this agenda.

Finally, Congress has continued to be active on leveraging the NTIB concept in legislation, by providing relief from duplicative security oversight to NTIB firms operating in the United States (see Appendix B for recent examples). Legislating on the efficacies of national interest determinations was an important step, but Congress and the administration should consider whether the current foreign ownership, control, and influence (FOCI) mitigation regime should be modified or abandoned, with respect to investments from trusted companies within the NTIB.

While progress has been made in beginning discussions on NTIB integration, much more needs to be done. The next section of recommendations outlines how the NTIB could be made more instrumental to solving US national security needs in the coming decades.

37 "Report to Congress Fiscal Year 2017 Annual Industrial Capabilities, Office of the Under Secretary of Defense for Acquisition and Sustainment," Office of the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base, March 2018, 15, https://www.businessdefense.gov/Portals/51/Documents/Resources/2017%20AIC%20RTC%2005-17-2018%20-%20Public%20Release.pdf?ver=2018-05-17-224631-340.

38 "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," 5.

Study Recommendations

The goal of this research is to provide the US Congress and the administration with a specific set of policy options for improving the NTIB. Many of these options are written in draft legislative language that can provide the basis for immediate consideration, either in the Fiscal Year 2020 National Defense Authorization Act or in 2019 administration policy and regulatory action. Perhaps, a more traditional study would be content with explaining the problem, and then outlining some generic policy proposals for discussion. Debate would hopefully ensue, more studies and hearings would be called for, and, perhaps within the next decade, modest change could be made that satisfies all parties with a stake in the issue.

However, the premise behind this work is that there is not enough time to do that. As with the urgent need to reform defense acquisition that began in 2015, the United States does not have the luxury of slowly pondering and making incremental changes to a Cold War management system that is no longer logical or practical, given the rapidly changing threat environment. To regain its place in world, the United States needs to leverage its allies and the commercial companies that reside in democracies to rapidly disrupt US adversaries. The first step is to begin establishing a trusted community to leverage current and future R&D, as well as existing and new production and manufacturing capabilities in the free world that are applicable to improving national security. That effort should start with the NTIB.

While much progress could be made through regulatory action, Congress may ultimately choose to pass legislation to provide greater urgency, intent, and guidance for needed reforms. The fact that Congress has been legislating on the NTIB in each of the last three NDAAs is a good start, and shows its continued interest in moving forward with the most trusted US allies. As a means of advancing change, a series of strawman proposals are put forth for consideration, with the knowledge that these will not be the final words on the subject. It is the hope that draft legislative language will save time, and is better to work with than a mere concept to spur debate. It is with that goal in mind that the following recommendations are put forth.

The study recommendations can be grouped into four categories that address: governance; technology-transfer reform; acquisition reform; and the further expansion of the industrial base. The ultimate goal is a step-by-step process leading to a harmonized NTIB defense free-trade area for goods, services, and—most importantly—ideas and research, within a defined, trusted community that will work to maintain the technology dominance of the United States and its closest allies. Each of these four categories of recommendations will be supported by a discussion of specific legal or regulatory proposals.

The first category of recommendations addressing governance is likely the easiest to implement, and is the one furthest along at the moment. It is always easy to create a new bureaucracy or discussion forum; it is much harder to create the right kind, which can adapt to the times and continuously adopt new practices. Since this is the easiest to implement, and the NTIB countries have already taken steps to begin talking, there is a risk that cooperation is likely to end here. That would be a serious mistake. Any such governance structure will require senior-leadership engagement, direction, and, probably, direct participation to establish the envisioned outcome, overcome the inevitable bureaucratic antibodies, and establish mechanisms to discuss and solve policy differences that deliver on the political imperative for a new approach.

The next recommendation in level of complexity and difficulty looks at technology-transfer reform. There is a risk that only cursory technology-transfer harmonization will take place, such as establishing a limited ITAR waiver (or more closely aligning inward-investment policies). These will not be sufficient to actually incentivize the types of R&D and cooperation needed across the NTIB. What is needed instead is a clearer vision, akin to that for the "Five Eyes" arrangement for intelligence, which enables freer sharing of innovation, technology and investment across these closest of allies—an equivalent "Five Eyes Defense Free Trade Zone." Broad and robust changes will be necessary to modernize technology-transfer laws, regulations, policies, and practices to establish the integrated defense-industrial base that US law calls for, to ensure the NTIB nations can work together—as they did to meet existential threats during World War II and in the first decades of the Cold War. They now need to respond to the far more complex threats they collectively face.

The third recommendation, addressing acquisition-process barriers, is probably even more daunting to implement. Fortunately, it is not as critical to addressing the threat as establishing technology transfer reform and

a governance structure to harmonize industrial policies across the NTIB. Still, acquisition-process differences will cause frictions within the NTIB that will eventually need to be addressed. For example, each NTIB country has established a series of socioeconomic programs around its defense budget and acquisition system that address domestic political concerns about obtaining domestic economic value for the expense of a dollar or pound on defense. In fact, even export-control policy may be evolving to serve more of a protectionist function than any real national security purpose. The recent Export Control Reform Act of 2018 provision, contained in the John S. McCain National Defense Authorization Act for Fiscal Year 2019—requiring that the impact on the national defense-industrial base be considered when ruling on any export-license application—may be a symptom of this evolution. A reciprocal harmonization of those socioeconomic barriers to participation—whether they are domestic source restrictions, small-business set asides, or offsets—are needed if any significant industrial integration is to be achieved. It is only after the implementation of these three categories of recommendations (governance, technology transfer, and acquisition reform) that a true defense free-trade zone within the NTIB can be established to serve as an engine of innovation and a new arsenal for the democracies of the world.

Finally, progress in the NTIB can set the stage for future integration between the NTIB countries and other close allies. NTIB reforms and the quadrilateral harmonization of industrial policy can serve as a test bed for future cooperative issues, where a next tier of allies could be brought in, either fully or on an *a-la-carte* basis.

Recommendation #1: Establish a governing body of NTIB members to address harmonization of industrial-base issues.

As described previously, progress has been made in forming a governance structure around the NTIB countries. This NTIB working group is a good start in recognizing that the four countries have a common industrial base, and that harmonized policies can help incentivize that base to better support the warfighters of each nation. Current NTIB strategic lines of effort in crosscutting enablers, industrial-base protection, small- and medium-enterprise integration, and human-capital-development integration are definitely areas where greater coordination is needed. It appears that improvements are being made in coordinating the review of foreign private investment and addressing risks to national infrastructure from Chinese information-technology communications-equipment firms. These improvements were inspired by recent US efforts to reform the processes and statutory rules of the Committee on Foreign Investment in the United States (CFIUS). NTIB nations are looking closely at how the United States will implement the Foreign Investment Risk Review Modernization Act (FIRRMA) to discern lessons and rules that may also apply to their foreign-investment security challenges.

Still, current NTIB infrastructure primarily comprises ad hoc panels working at relatively low levels of the bureaucracy. There is a need for greater formality and continuity of this process, as well as conducting discussions and focusing decisions at a higher level. While the deputy assistant secretary of defense (DASD) for industrial policy in the Office of the Under Secretary of Defense, Acquisition, and Sustainment is spearheading this effort for the United States, the downgrading of that position in the last ten years to two levels below an undersecretary has made it more difficult to lead than it should. This position should either be upgraded to an assistant secretary or returned to the deputy undersecretary level, to provide more authority within the US interagency structure on these issues. It is helpful that a political appointee should lead this effort in the United States, but it still risks being overcome by changes in personality or government. Ideally, decision authority for the US delegation to an NTIB Quadrilateral Group should be held at least at the deputy secretary level, with undersecretaries providing guidance to working groups headed by assistant secretaries. If the United States established leadership at this level, there is little doubt that other NTIB countries would reciprocate with equivalent senior-level personnel. This is especially pertinent given the large role that the DASD for industrial policy has in the CFIUS process—a role that has now doubled with the passage of the FIRRMA legislation.

The goal of any future NTIB Quadrilateral Group should be to harmonize industrial policy across the NTIB countries, and to share best practices in acquisition and industrial management. Key areas ripe for cooperation include: industrial security/security of supply chain; cybersecurity (both within the governments and in the industrial base, to include critical-infrastructure protection); regulating foreign direct investment through CFIUS-like mechanisms; and using foreign ownership, control, and influence (FOCI) mitigation to address foreign influence in the NTIB. Discussions in this grouping will hopefully help guide the FIRRMA implementation, as the United States seems to be making a mistake by not calling out those nations that do not play by

the rules. The net result may be a foreign-investment regime that makes it more difficult for allies to invest in the United States, while the Chinese and Russians continue to find other ways to steal intellectual property and divert technology through well-placed assets in companies, investments, joint ventures, and partnerships. Technology transfer and control, as well as foreign-defense-sales practices, should be additional topics for discussion, along with the need for addressing acquisition-process barriers.

In the area of harmonizing acquisition oversight, Australia and the UK may want to consider establishing an entity similar to the Canadian Commercial Corporation to address reciprocity in pricing issues with the United States, and to make it easier for small businesses to access the NTIB. Finally, and most importantly, a more robust sharing of market research and technology assessment is needed, to allow for greater coordination and maximization of scarce R&D resources. This would include not only government-sponsored research, but also university and corporate research, and a greater understanding and leveraging of venture-capital and private-equity investment. As the NTIB Quadrilateral Group becomes more mature, the agenda could evolve to address additional industrial-policy issues that could better address the security threats arising from a resurgent Russia and China, as well as proliferation threats from Iran and North Korea.

There is also likely a need for a dispute mechanism within the group. Many of the areas for regulatory and legal harmonization will be subject to differences and interpretation. There should be a process to bring up issues for discussion and challenge on a fairly routine basis. A working group oversight body comprising representatives of the four NTIB governments may need to be established to oversee the implementation and execution of agreed changes, and to serve as the first level of arbitration on any program-specific or policy disputes that arise. Such a body may be useful in discussing current differences in evaluating the threat of, say, Huawei technologies to national infrastructure in wartime.

While a senior NTIB governance structure could be established through existing authorities, Congress may choose to provide greater legal formality, continuity, and certainty. The following provision is one way to establish such an entity in law, and to initially set the agenda for NTIB cooperation by folding the requirement into the original NTIB legislation.

Legislative Proposal 1A:

Establishment of National Technology Industrial Base Quadrilateral Council

(a) AMENDMENT TO TITLE 10, UNITED STATES CODE.—Section 2502 of title 10, United States Code, is amended by inserting after subsection (d) the following:

(e) (1) The Chairman of the National Defense Technology and Industrial Base Council shall work with the equivalent designees in the countries that comprise the National Technology Industrial Base to form the National Technology Industrial Base Quadrilateral Council.

(2) The National Technology Industrial Base Quadrilateral Council shall meet biannually to harmonize respective policies and regulations, and to propose new legislation that increases the seamless integration between the persons and organizations comprising the national technology and industrial base (as defined in section 2500 of title 10, United States Code).

(3) The National Technology Industrial Base Quadrilateral Council shall:

> **(A) address and review issues related to industrial security, supply-chain security, cybersecurity, regulating foreign direct investment and foreign ownership, control and influence mitigation, market research, technology assessment, and research cooperation within public and private research-and-development organizations and universities, technology and export-control measures, acquisition processes and oversight, and management best practices; and**
>
> **(B) establish a mechanism for National Technology Industrial Base Quadrilateral Council members to raise disputes that arise within the national technology industrial base at a government-to-government level."**

This proposed legislative provision would amend section 2502 of title 10, USC, and require the secretary of defense—who is designated in law to serve as the chairman of the National Defense Technology and Industrial Base Council—to establish a National Technology Industrial Base Quadrilateral Council group. This group would periodically meet to harmonize respective policies and regulations, and to propose new legislation that would increase the seamless integration between

the persons and organizations comprising the national technology and industrial base. This provision would also establish a minimum agenda for the NTIB Quadrilateral Council to address, and require a disputes mechanism for NTIB council members to address differences in implementation of policies.

The goal of this provision would be for NTIB members to harmonize international agreements, laws, regulations, and practices. Obviously, US law cannot bind partner countries, but it does not appear that any of the NTIB allies would object to greater formality and continuity in NTIB governance. While US law cannot compel other countries to meet, having this body in statute would provide a greater legitimacy and staying power, and would allow Congress to push any reluctant future administration to continue progress toward greater integration. The NTIB member nations have frequently noted a need for a government process for addressing issues that arise during NTIB transactions and desired transactions.

Recommendation #2: Harmonize technology-transfer laws, regulations, policies, and practices to establish an integrated defense-industrial base

Implementing the right kind of export-control reform is probably *the* most important management-process improvement effort that the United States needs to address in the immediate future, if it wants to succeed in any future innovation competition with China and other near-peer competitors. Getting this issue wrong will set the United States and its allies back decades in any future conflict. The United States needs to not only scale industrial capacity, but to incentivize creative solutions in both the traditional defense-industrial base and the nontraditional industrial base. It needs to stop incentivizing companies from moving R&D offshore or developing products first for the commercial market to avoid the perils of the current ITAR system.

The NTIB is the ideal testing ground for any such export-control reforms, as it will allow the United States to expand its defense-industrial capabilities within a trusted community of both traditional and nontraditional contractors. Making it easier to cooperate with the UK, Australia, and Canada provides some much-needed scale to the US defense-industrial base, but each country is also home to many of the types of commercial companies needed to address future US national security problems. The NTIB provides a relative "safe space" for technology-transfer reform where rules, incentives, standards, practices, and cooperative measures can be tested to get them right within a cultural framework of cooperation that has been in existence for more than one hundred years. If the United States cannot reform its export controls within this group, it has no real hope of doing so in any other forum, or with any other nation.

The following proposals address two alternative export-control-reform approaches within the NTIB, although some ideas within each may be complementary. The first approach is to establish a robust ITAR waiver that would be granted to all countries in the NTIB, with an explanation of what that waiver should look like in practice, as any such waiver should be much different than the current Canadian ITAR exemption. The second approach lists those reforms that could be implemented in the absence of a full NTIB ITAR waiver. Regardless of the approach taken—whether a blanket ITAR waiver or what would, in a sense, be a series of robust program licenses in wide-ranging technology areas—the key aspects necessary to each approach are: the establishment of a trusted community to include the US industrial base, operating under the same rules; addressing the issues of the ITAR taint and extraterritoriality by controlling items at the end-item level and trusting NTIB partner nations' export controls; exempting cooperative research-and-development activities from triggering application of the ITAR; and controlling technologies based on their classification level.

NTIB Export Control Reform Recommendation Approach #1: Establish NTIB ITAR Exemption

This category of NTIB export-control proposals revolves around the establishment of an exemption to ITAR for the NTIB countries. As Canada already has such an exemption, step one would be to merely apply this exemption to Australia and the United Kingdom. This has the utility of ease of implementation. This will not achieve the "seamless integration" of the NTIB called for in the law, as to do that will require several changes to the Canadian waiver, but it is the necessary first step to begin the process of including the UK and Australia in the NTIB.

> **Action Required: Expand ITAR §126.5 "Canadian Exemptions" to include the UK and Australia.**

The Canadian ITAR waiver was, in essence, a legacy fact on the ground when the ITAR was created in the mid-1970s, and was much broader than the current waiver. The Canadian ITAR exemption was significantly

narrowed in the early 2000s to address technology diversion to Iran, which led to the establishment of a Canadian Controlled Goods Program for the handling of unclassified ITAR information.

There is some debate among those interviewed about whether statutory change is necessary to apply this same waiver to the UK and Australia. One possible interpretation is that the current Canadian exemption is essentially an existing "performance" exemption from the ITAR, which was recognized when the Arms Export Control Act of 1975 was enacted. Corresponding legislative language exists in title 22 of the United States Code to recognize that waiver in law. A similar performance waiver for the UK and Australia could be established by a regulatory change to the ITAR, and the law could ideally be modified to reflect that fact. During the course of this study, there were indications that US government representatives expected the NTIB implementation plan to result in the expansion of the current Canadian ITAR exemption to include the UK and Australia—but, to date, that has not been proposed.

While expanding the ITAR waiver can probably be done administratively, the following two legislative-language proposals would allow Congress to conform the law to whatever ITAR waiver may be put forward by the administration. One would address just the UK and Australia, while the other option would be written to address the NTIB countries, so that any countries added in the future would automatically qualify for the waiver, which would meet the intent of the original legislation. The following legislative proposal would conform statute by adding the UK and Australia to the existing Canadian ITAR waiver.

Legislative Proposal Option 2A:

Licensing Exemption for the United Kingdom and Australia

(a) In General.—Section 2278(f)(3) of title 22, United States Code, is amended by inserting ", the United Kingdom of Great Britain and Northern Ireland, and Australia," after "Canada".

(b) Conforming Changes.—Section 2278(j)(1)(B) of title 22, United States Code, is amended to read as follows—

> **(1) Exception for Canada, the United Kingdom of Great Britain and Northern Ireland, and Australia**
>
> **(2) The requirement to conclude a bilateral agreement in accordance with subparagraph (A) shall not apply with respect to an exemption for Canada, the United Kingdom of Great Britain and Northern Ireland, and Australia from the licensing requirements of this chapter for the export of defense items.**

(c) Conforming Repeal—Section 2278(j)(1)(C) of title 22, United States Code, is repealed.

==========

This second legislative proposal would conform statute to an NTIB waiver, rather than specifically listing Canada, the UK, and Australia. This approach is preferable, as it has the advantage of addressing any future expansion of the NTIB.

Legislative Proposal 2B:

Licensing Exemption for Countries Comprising the National Technology Industrial Base

(a) In General.—Section 2278(f)(3) of title 22, United States Code is amended by striking "Canada" and inserting countries comprising the national technology industrial base, as defined in section 2500 of title 10, United States Code.

(b) Conforming Changes.—Section 2278(j)(1)(B) of title 22, United States Code is amended to read as follows—

> **(1) Exception for Countries Comprising the National Technology Industrial Base**
>
> **(2) The requirement to conclude a bilateral agreement in accordance with subparagraph () shall not apply with respect to an exemption for countries comprising the national technology industrial base, as defined in section 2500 of title 10, United States Code, from the licensing requirements of this chapter for the export of defense items.**

(c) Conforming Repeal—Section 2278(j)(1)(C) of title 22, United States Code, is repealed.

==========

If the administration does not act in the next few months to enact an NTIB ITAR performance waiver, Congress could also consider strongly recommending that the president exempt the UK and Australia from ITAR.

Legislative Proposal 2C:

Licensing Exemption for the United Kingdom and Australia

The committee directs the president to consider exempting the United Kingdom of Great Britain (UK) and Northern Ireland, and Australia in a manner similar to the exemption for Canada found in section 126.5 of the International Traffic in Arms Regulations. The committee notes that since the U.K. and Australia have been added by law to the National Technology and Industrial Base, as defined in section 2500 of title 10, United States Code, these countries should also receive the same exemption that Canada enjoys under section 126.5 of the International Traffic in Arms Regulations (22 CFR 120-130).

==========

If an ITAR waiver is established for Australia and the UK, it is essential that it include certain revisions to maximize its effectiveness. If the expansion of the NTIB leads to an ITAR waiver for the UK and Australia, it would be a significant first step, but it is important to address what type of waiver is necessary to maximize the benefits of a larger industrial base. To allow for what would essentially be a defense free-trade zone between the four countries, the first step, paradoxically, is to narrow the definition of who is allowed into this export-license-free zone. The establishment of this community provides reassurance that designated entities can be trusted to handle what is, in essence, a separate level of classified information for the United States, even though most of the information involved is not classified.

> **Action Required: Establish a trusted community for ITAR license-free transfers based on a reciprocal recognition of entities holding security clearances in the United States, Canada, the UK, and Australia and for those companies without a security clearance, adopt a version of the Canadian Controlled Goods Program or the US-Canada Joint Certification Program in the rest of the NTIB.**

A trusted community could be established through regulatory implementation of an ITAR waiver for the NTIB countries. There is, of course, a significant tradeoff with this concept. On one hand, it potentially limits the companies that may innovate on one country's behalf; on the other, it is a necessary evil in ensuring that the benefits of the flow of restricted information or technology does not apply to those who should not be trusted to handle them (e.g., Chinese, Russian, or Iranian front companies). There are many ways to define a trusted community, and this section proposes a couple of options. The key issues are to establish such a community, address who should be in it, and define by what criteria one should trust entities within that community.

The Defense Trade Treaties with the UK and Australia got it right with respect to the first cut of who should be a part of any trusted community, by establishing reciprocal recognition of companies with security clearances.[39] Even though the vast majority of ITAR information is unclassified, it has become its own de facto security classification. It is controlled information, and companies that understand how to control classified information should more easily be trusted to control less-sensitive, unclassified information.

Defense companies, both within the United States and abroad, already control ITAR information through their security-control bureaucracy, just as if ITAR were a classified document or technology and, as such, should be the foundational basis for the trusted community. If it were not for the fact that most ITAR information is unclassified, it would make complete sense to just classify all ITAR information at the Secret level and control it that way, rather than through export-control licenses. Those companies trusted with a security clearance already know how to protect information however it is marked, and it is extremely difficult to do business within the defense-industrial base without a security clearance.

There is some experience in trying to establish regimes for the reciprocal recognition of security clearances that could be leveraged. The first is the List X group of companies established in the UK to implement the US-UK Defense Cooperative Treaty, and the second is the similar list that Australia has created to implement its treaty obligations. Some believe that the registration process for List X is too costly and burdensome, and that is probably true. As with much of the treaties, it is probably better just to scrap the mechanisms and start over, but the concept of establishing a list of cleared companies to obtain access to ITAR

39 One issue with the treaties, which must be addressed in any future reform effort, has to do with these criteria. What happens to companies that want and need to be a part of the approved community, but don't have a security clearance, and don't really want or need one because the ITAR information is unclassified? A lesson from this experience is there should be a path to join the trusted community without having a security clearance.

information without a license is one that still should be pursued.

Rather than use the UK's List X and the Australian list, the recommended approach is to establish a Quadrilateral Security Clearance List that US, Canadian, Australian, and UK firms could register with their respective security agencies, which would be the basis for the initial reciprocal recognition of clearances and access to the ITAR-exemption trusted community. Registration for this list should be as easy to comply with as the US-Canada Joint Certification Program, which allows Canadian firms to take advantage of its limited ITAR waiver and compete on an equal basis with US firms.

Expanding the concept of the existing US-Canada Joint Certification Program (JCP) to include the United Kingdom and Australia, and limiting it to cleared firms, would allow contractors in all four countries to apply for favorable treatment for sharing of export-controlled technical data and critical technology. This program reduces the export-control burden on data, requirements, and solicitation information, which currently allows Canadian firms (and would enable British and Australian firms) to compete for business on equal footing as US firms, and would be a significant step toward the overall objective of license-free transfers within the NTIB. The disadvantage of just adopting the JCP is many Canadian firms are not currently cleared, but it is possible to take the JCP, change the criteria for registration to only firms holding a clearance, and expand the program to Australia and the UK.

The JCP discussion leads to the issue that not all companies that should benefit from an ITAR exemption will be traditional defense contractors with security clearances. The lesson learned from the original, broad Canadian ITAR exemption was that within any license-free zone, a trusted industrial community would need to be established to prevent foreign-national front companies from taking advantage. The first such trusted community established in reaction to foreign subterfuge to evade export controls in the 1990s was the Canadian Controlled Goods Program (CGP), established in 2001 as mandated in the Canadian Defense Production Act.

The Canadian Controlled Goods Program addresses unclassified ITAR-controlled transfers within Canada. It requires companies receiving ITAR-controlled materials to register with the Canadian government and be subject to certain compliance-assurance requirements. Registration under Canada's CGP requires the security assessment of designated company officials, and may entail a compliance inspection to ensure that the company adheres to basic security standards for receipt and handling of controlled goods. The Joint Certification Program currently addresses some transfers that primarily encompass the transfer of knowledge (TAAs or Technical Assistance Agreement) to allow for Canadian firms to bid on US work. The Controlled Goods Program and the Joint Certification Program (as modified to address a separate classified list, as proposed above) should be the models for establishing the trusted NTIB community for those companies that choose not to have a security clearance. These two programs could be a stepping stone for nontraditional companies to a security clearance, but it should be enough to be a part of the trusted community to support defense programs at an unclassified level.

While UK and Australian firms without a security clearance could become a part of the NTIB trusted community, through the creation of a similar controlled-goods program, the United States is the weakest link as far as ITAR security—and probably has been for decades. One weakness of the US technology-transfer system of the past decades is the focus on the establishment of foreign processes of control, such as the controlled-goods program in Canada, while the United States had no trusted community equivalent. The United States has been a massive internal free-trade zone for sensitive technologies—one of which foreign adversaries have been able to creatively take advantage, just as they once used Canada. One finding of this study is that the Canadians have created a system that can work for controlling the internal transfer of sensitive goods and services, and also gives their government a full picture of the threat profile for these sensitive items. This is better than what the United States has, which is nothing more than basic legal compliance and hoped-for legal enforcement. As long as one is a US citizen or US company, there are no checks on receiving ITAR information, as long as it is transferred within the United States—despite constant reminders that not all US citizens and corporations can be trusted to obey the law.

The problem for US adversaries that gain access to technology within the US border is how to get it out. This may be as easy as carrying it out on a thumb drive or, better yet, leaving a backdoor on a US consumer's computer open for hackers in Xian to download files. While there have been a growing number of Department of Justice cases addressing this kind of theft, those are likely only a fractional indicator of how much technology is actually leaving the country. The United States should consider establishing a CGP similar to what exists in Canada to address this problem,

although it would need to get over the hypocrisy it has shown in its treatment of Canada—as when it narrowed its ITAR waiver twenty years ago. US controls are not in any way superior to the controls of allies; in fact, they are a source of a technology-leakage problem far greater than those of allies.

Legislative Proposal 2D:

Establishment of a US Controlled-Goods Program

(a) Report Required. —Not later than 260 days after the date of enactment of this Act, the Secretary of Commerce and the Secretary of Defense shall jointly report to Congress on the advisability and feasibility of establishing a program internal to the United States for the control of unclassified sensitive goods and knowledge similar to the Controlled Goods Program established by the Government of Canada.

==========

Once a trusted community is established, the issue becomes what to protect. Protect too much, and the supply chain grinds to a halt. If the United States were to establish an internal controlled-goods program, it would provide an opportunity to change the criteria for what is protected, as it is likely US firms would push back on the establishment of any new controls. Ideally, whatever new trusted community was established would create higher walls around fewer things and, for everything else, establish a license-free area for cooperation. Still, there will be some technologies that should be excluded from any license-free zone, as each country may not wish to share some of its "crown jewels" with its NTIB partners. The answer is not to create broad categories of excluded technologies, as is the case with the Canadian ITAR exemption and the Defense Trade Treaties, which provide an excuse to broadly control technology unnecessarily. The easiest solution is to control technology and knowledge by classification levels, and limit access to technologies through a Top Secret classification level that would require traditional export-control licenses.

Action Required: Excluded technologies from any NTIB ITAR exemption should be based on the classification of the defense item or service, and be classified at the Top Secret level

Within the NTIB trusted community of four nations, license-free transfer of goods, services, or knowledge would be authorized based on the classification of the good, service, or knowledge. Currently, there are exempted technologies that are not eligible for export under either the Canadian exemptions or the treaties. The Exempted Technologies List has long been cited as a major impediment to use of the Defence Trade Treaties. Rather than adjust the lists, it might be better to focus control on classification, and to classify any technology a country wants to exempt as Top Secret. This would correspond to these technologies being the most sensitive technologies and programs of each country, and would focus attention on those that are truly vital to national security.

Thus, two free-trade zones would be established at both the unclassified level with CGP and cleared entities, and then at the classification level of Confidential and Secret for cleared entities. There is the expectation that some technologies will still want to be controlled by NTIB countries. These should be classified Top Secret, and either a new or existing export-control licensing procedures should be in place for those technologies exempted from a license-free zone. Congress could recognize this approach by putting a limitation on license-free trade at the Top Secret level.

Legislative Proposal 2E:

Excluded Technologies

(a) In General.—There shall be an exemption to the International Trafficking in Arms Regulations for countries comprising the National Technology Industrial Base that allows for license-free trade that shall only apply to defense articles and services classified at the Secret, Confidential, Sensitive but Unclassified, and Unclassified levels.

(b) Secretary of Defense Review.—The Secretary of Defense shall review any sensitive technologies and programs that should be exempted from license-free transfers within the National Technology Industrial Base and after identification shall control those technologies and programs at the Top Secret level.

(c) Report Required.—Not later than 260 days after the date of enactment of this Act, the Secretary of Defense shall provide to the Committees on Armed Services in the Senate and House of Representatives, the classified list of sensitive technologies and programs that the Secretary determines should be exempted from license-free transfers within the National Technology Industrial Base.

==========

The next issue to address after establishing an NTIB ITAR exemption defining the trusted community and addressing the application of the ITAR exemption, including what is excluded, is to eliminate application of the concepts of the ITAR taint and extraterritoriality.

Action Required: Control of transfers outside the NTIB for defense goods and services originating within the NTIB that are not classified at the Top Secret level should be at the end-item level, with export controls for components and subcomponents within the defense item, will be under the jurisdiction of the host government where final manufacturing takes place or will perform the defense service.

Even with the most expansive ITAR exemption under US export controls, there will still be a legacy issue of tracking anything that could be transferred outside the NTIB sphere. The paperwork requirement to track any license-free transfers within the NTIB would not go away, because of the fear that anything exported from the NTIB countries could be transferred to a third country. The bureaucracy to do this would be enormous, and completely unproductive. Currently, the UK, Australia, and Canada control technology on an end-item basis and, once a decision is made to transfer this technology to another foreign country, control for the item ends. With its focus on knowledge and extraterritorial controls, the United States continues to follow every interaction with US technology or US citizens as a means of control—thus, the source of the infamous ITAR taint. For the NTIB to be truly integrated, the United States needs to trust the NTIB countries not to transfer technology to countries when it is not in their national security interest to do so. Thus, the ITAR taint and extraterritoriality application should be eliminated within the NTIB ITAR exemption. This will likely bring about disagreements over specific cases of exports to certain countries, but a system of open transparency and discussion within the NTIB Quadrilateral Group about the export of end items would be a mechanism to address future sales and foreign policy disagreements that may arise regarding proposed technology transfer beyond the NTIB.

The following legislative proposal would achieve these goals.

Legislative Proposal 2F:

Extraterritorial Applications Within National Technology Base License of Free Transfers of Applicable Technology

(a) Notwithstanding section 2278 of title 22, defense articles and defense services classified at the Secret, Confidential, and Unclassified levels may be transferred within the National Technology Industrial Base shall be controlled at the end-item level.

(b) Notwithstanding section 2278 of title 22, the further transfer or retransfer or maintaining of defense articles, whether an end-item, component, subsystem, or technical knowledge, or defense services when transferred from the United States to a country that comprises the National Technology Industrial Base shall be regulated and controlled by the country within the National Technology Industrial Base where the defense article resides, regardless of whether such article or service is of United States origin or whether such article or service contains United States-origin components.

NTIB Export Control Reform Recommendation Approach #2: Non-ITAR Exemption Options

The following category of recommendations would address export-control reforms in the absence of an ITAR exemption for the NTIB countries.[40]

The first proposal is a minimalist approach that would address the most contentious issues raised by US partner nations. This proposal would reduce the bureaucracy involved in third-party transfers, which is primarily caused by the outsourcing of systems maintenance to the private sector. While this option essentially treats allies like grown-up countries who can manage their supply chains, and allows them to better support US military operations, it does nothing to incentivize the types of research-and-development cooperation that is needed in the future—but at least it is a step in the right direction.

Legislative Proposal 2G:

Post-Export Supply Chain Transfers Within National Technology Industrial Base Countries

40 Several of these proposals are modified versions of proposed Senate amendment number 4575 to S. 2943, to authorize appropriations for fiscal year 2017 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy that was introduced by Senator John McCain in the 114th Congress. This amendment was not brought up for debate, and was not included in the final act.

(a) In General.—The government of a country that is part of the national technology industrial base, as defined in section 2500 of title 10, United States Code, may transfer United States-origin material within that government's supply chain without further United States Government approval or the need to comply with additional export-licensing requirements, provided that the material remains in the ownership of such government.

This could also be done administratively, without legislation, by revising ITAR section 126.5 to allow transfers among qualified nongovernmental entities. This proposal would ease retransfer requirements to facilitate maintenance, repair, installation, and integration, and would meaningfully reduce the burden of export controls. NTIB governments would be authorized to transfer material from another NTIB partner within the receiving country's own supply chain, without the need for additional licensing requirements. The NTIB could also enable greater supply-chain integration by allowing a company with facilities in two or more NTIB countries to transfer controlled material between facilities without the need for an export-control license.

==========

While the above proposal would address end items, the most important national security imperative is to get the NTIB Science, Technology, Engineering, and Math (STEM) workforce talking to one another. The following proposal would essentially establish a TAA free zone within trusted companies that conduct operations in several NTIB countries. This would address the current inability of scientists and engineers within the same company to talk to one another to solve defense problems, without the State Department providing upfront permission.

Legislative Proposal 2H:

Integration of Supply Chain Within National Technology Industrial Base.—

(a) In General.—A company included on the list under paragraph (b) with facilities in both the United States and in a country that is part of the national technology industrial base, as defined in section 2500 of title 10, United States Code, may transfer controlled material to include material governed by technical-assistance agreements between a United States facility and its other facilities located in a national technology industrial base country without the need for United States Government approval or the need for an additional export-control license. Any such transfer must comply with United States security classification requirements.

(b) Approved Company List.—The list referred to in paragraph (a) is a list maintained by the Secretary of Defense and the Secretary of State of companies and facilities the Secretaries have determined are qualified for the streamlined transfer authority under such paragraph.

While this would allow for subsidiaries of companies to talk to one another, the next step would be to broaden this TAA-free zone to allow for discussions to take place between different companies within a trusted community of companies.

Legislative Proposal 2I:

Integration of Supply Chain Within National Technology Industrial Base

(a) In General. —A company included on the list under paragraph (b) with facilities in a country that is part of the national technology industrial base, as defined in section 2500 of title 10, United States Code, may transfer controlled material to include material governed by technical-assistance agreements between facilities located in a national technology industrial base country without the need for United States Government approval or the need for an additional export-control license. Any such transfer must comply with United States security classification requirements.

(b) Approved Company List.—The list referred to in paragraph (a) is a list maintained by the Secretary of Defense and the Secretary of State of companies and facilities the Secretaries have determined are qualified for the streamlined transfer authority under such paragraph.

==========

In the absence of an ITAR exemption for the UK and Australia, it is possible to try fixing the Defense Trade Treaties, although it is debatable whether it is worth the effort. One of the most significant barriers in the treaty is the Exempted Technologies List, which, as currently constituted, includes too many items. The list could be scrubbed and the trusted community could be more broadly defined—but, because of the history of the treaties' implementation of the treaties—this may not be as efficient as other measures.

Legislative Proposal 2J:

Implementation of Treaties on Defense Cooperation.

(a) In General.—The Secretary of State and the Secretary of Defense shall conduct a joint review of the exempted technologies lists that apply to the Treaty Between the Government of the United States of America and the Government of Australia Concerning Defense Trade Cooperation, signed in Sydney on September 5, 2007, and the Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defense Trade Cooperation, signed in Washington and London June 21 and 26, 2007, with the aim of reducing the applicable lists to the minimum compatible with international obligations.

==========

A program-licensing/global-project-authorization approach has been a discussion topic with the United States for decades, but with very little progress made in establishing such a scheme. The Defense Trade Treaties were designed to obviate the need for such a licensing vehicle, but, with limitations on the use and effectiveness of the treaties, a program license or project authorization could be an effective option to allow for license-free trade among qualified NTIB contractors across the life of a project or program.

Program licensing has been a key export-reform proposal since the 1990s, and has been resurrected as a new recommendation for NTIB integration.[41] One observer remarked that: "ITAR §126.14 theoretically allows US applicants the ability to apply for project or program licenses although in practice, these devices are seldom if ever used, anecdotally due to liability concerns among US exporters."[42] In other words, the risk from the compliance burden placed on any of the proposals by the State Department has made US companies decide not to bother. Until the State Department bureaucracy embraces program licenses, it is likely this risk averseness on the part of US companies will not go away. Still, a program license or global project authorization would capture the advantages of license-free trade, and is a potentially effective means of mitigating burdens of ITAR compliance on complex projects or programs.

As with many export-control reforms, the problem is there seems to be a lag time of about twenty years from when a proposed reform should be enacted, and when it actually happens. Unfortunately, the world has been moving on since the concept of program licensing was proposed, to very little effect, in the 1990s. Many future industrial efforts will not address individual programs, but will instead address capabilities of systems. To really benefit from the industrial cooperation, a program license should account for cooperation among several different programs that contribute to such a capability. Thus, for a program-licensing regime to be effective in this new environment, it should actually be a capabilities licenses—i.e., there should be a broad category of program licenses geared to creating certain capabilities. Within that license, there should be an identified group of companies within each country, but also the ability to clear a new company into the license without the current wait time of six to nine months.

Legislative Proposal 2K:

Enhanced Program Capabilities Licensing.

(a) In General.—Not later than one year after the enactment of this Act, the Secretary of Defense and the Secretary of State shall establish a structure for implementing a revised program export licensing framework with the countries comprising the national technology industrial base, as defined in section 2500 of title 10, United States Code.

(b) Elements.—(1) Program licenses should cover broad categories of capabilities and may involve more than one acquisition program.

(2) Except under exceptional circumstances, all defense articles transferred within the national technology industrial base to include items sold under the foreign military sales program shall be governed by a program license which shall allow for unrestricted transfers and retransfers in accordance with the technology control structures of the receiving nation of the national technology industrial base.

==========

The following proposal addresses the need for nontraditional companies that are currently working on commercial products and services not to be tainted by ITAR once they begin working on a defense project. This parallels the commercial-item definition currently in US statute for the non-application of noncommercial

41 See March 2018 CSIS NTIB report referenced above.

42 Email interview with author.

acquisition clauses.[43] The application of the ITAR is essentially a noncommercial, government-unique requirement that is currently placed on commercial products and services once they are tainted with US defense R&D funds. Defining something as a commercial item allows not only for the original commercial, off-the-shelf product to be exempt from ITAR, but also modifications and products that are of a type or similar to a product developed by the commercial-item provider. This would address the danger of an item getting tainted by ITAR. This proposal would be useful in enticing nontraditional players who currently do not want to participate in the defense-industrial base because of a fear of losing access to their intellectual property and commercial use. This would apply to firms throughout the NTIB.

Legislative Proposal 2L:

National Technology Industrial Base Commercial Item International Traffic in Arms Regulation Exemption.

(a) In General.—Any commercial item, as defined in section 103 of title 41, United States Code, that originates in a country that is a part of the national technology industrial base, as defined in section 2500 of title 10, United States Code, and incorporated in a defense product shall be regulated under the Export Administration Regulations (part 730 of title 15, Code of Federal Regulations) is exempt from regulation under the International Traffic in Arms Regulations (subchapter M of chapter I of title 22, Code of Federal Regulations).

There are some issues with a commercial-item ITAR exemption as it relates to any of the 600 series items that were transferred from State Department to Commerce Department jurisdiction the issues of the ITAR Taint and extraterritoriality have transferred themselves with the transfer of jurisdiction. This issue still needs to be reviewed and resolved, and the NTIB countries may eventually need to be treated differently within the 600 series. Once this provision is established in law, one option to consider addressing the ITAR taint for products supplied by NTIB countries is to deem any defense items and services provided by an NTIB country to the United States as commercial items subject to the above exemption.

==========

The Foreign Military Sales Program is a separate problem within the NTIB. It is its own separate system, with its own level of controls that are different from those under the ITAR or Commerce jurisdiction. All of this should be harmonized. The inconsistency in controls between Direct Commercial Sales and FMS following recent export-control reform is a major challenge for non-US companies in complying with US export controls. Third-party transfers of FMS items should be subject to the control regime of their appropriate product jurisdiction—Department of Commerce or Department of State—rather than see the creation of new, onerous restrictions attached to FMS programs contained in a letter of offer and acceptance (LOA). While eventual statutory harmonization may be more complex than what is proposed here, the following is at least a start for identifying what changes in the law are necessary to harmonize ITAR, the Commerce Control List, and FMS.

Legislative Proposal 2M:

Foreign Military Sales Harmonization with Other Technology-Transfer Regimes.

(a) In General.—The Secretary of Defense, Secretary of Commerce, and Secretary of State shall ensure that items transferred under the Foreign Military Sales Program to countries belonging to the national technology industrial base, as defined in section 2500 of title 10, United States Code, shall not be subject to technology-transfer controls in excess of those than exist under the International Trafficking in Arms Regulations or Export Administration Regulations.[44]

==========

Another issue that repeatedly surfaces is that NTIB countries are being forced into using the FMS program to buy US systems. This is not unique to NTIB countries, but the reality is these countries have more sophisticated acquisition and purchasing capabilities, and are better able to negotiate directly with a US contractor. Regardless, the FMS requirement results in the NTIB countries facing greater complexities of adhering to a different technology-transfer regime, rather than giving these countries the option to buy US systems through a direct commercial sale regulated under ITAR. In the absence of harmonization of the ITAR with FMS, another proposal would be to grant the NTIB nations the right to choose and directly negotiate with US suppliers.

43 See Section 2375, title 10, United States Code.

44 An "in excess of" standard may prove difficult to measure; another approach to consider may be to explicitly state that only ITAR/EAR

Legislative Proposal 2N:

Treatment of National Technology Industrial Base Under Foreign Military Sales Program

(a) In General.—Countries comprising the national technology industrial base, as defined in section 2500 of title 10, United States Code, may purchase items traditionally availably as foreign military sales items under a direct commercial sale, and not be required to purchase defense items from the Foreign Military Sales Program.

==========

Action Required: Continue reforms as applied to the NTIB to further seamless integration and promote cooperative research and development and production of defense capabilities

Additional export-control and technology-security reforms within the NTIB will be necessary as the full integration of the new NTIB countries continues. Just as Congress recently addressed the issue of national interest determinations within special security agreements of firms that are part of the NTIB, additional modifications—or even the abolishment of FOCI mitigation for trusted firms under the NTIB—should be considered. The following proposal would provide a formal role for the secretary of defense, working with the National Defense Technology and Industrial Base Council to focus on additional export-control reforms and technology-security reforms within the NTIB. This proposal could be enacted no matter what approach the administration took on these activities within the NTIB, and this legislative proposal would ensure that discussions on these issues would have, at a minimum, a forum to take place without further legislative or administrative action.

Legislative Proposal 2O:

Plan for Implementation of National Technology Industrial Base Reforms

(a) Report Required.—The National Defense Technology and Industrial Base Council shall report to the congressional defense committees no later than 180 days following the passage of this act, a plan to provide for the seamless integration of the transfer of defense goods and services to include the nature of export-licensing exemptions and technology-security reforms within the countries comprising the National Technology Industrial Base to meet the objectives set forth in the National Security Strategy Report submitted to Congress by the President pursuant to section 108 of the National Security Act of 1947 (50 U.S.C. 3043) and the policy guidance of the Secretary of Defense provided pursuant to section 113(g) of title 10, United States Code.

==========

Recommendation #3: Limit Socioeconomic and Acquisition Process Barriers to Cooperation, to the Maximum Extent Practicable

Harmonization of industrial policies and lowering export-control barriers will further NTIB cooperation and innovation and the creation of new defense products. Additional measures will be needed to actually get each country to buy each other's products, or to expand competition within the NTIB. The key barriers that have been cited as problems have been domestic-source restrictions, offsets in Canada, the UK, and Australia, and small business set-asides and percentage goals for socioeconomic programs in the United States. The following legislative proposal would allow for the secretary of defense to negotiate and establish reciprocity with the NTIB countries in these areas.

Legislative Proposal 3A

RECIPROCITY IN SOCIOECONOMIC PROGRAMS WITHIN THE NATIONAL TECHNOLOGY INDUSTRIAL BASE

(a) In General.—The Secretary of Defense may waive any domestic source restriction or small-business provision in law to further the seamless integration between the United States and a country within the national technology industrial base if the Secretary certifies that a country within the national technology industrial base will—

(1) not engage in offsets with respect to a U.S. sales of defense items;

(2) provide open access to U.S. defense goods and services that are not inhibited by legislated or regulatory domestic source restrictions that preclude the sale of a U.S. item; and

rules should apply to FMS cases.

(3) treat U.S. small businesses the same as domestic small businesses.

==========

With regards to US domestic-source restrictions, many of these are already waived under the Reciprocal Defence Procurement Memorandum of Understanding (MoU) agreements the United States has with the NTIB countries. An issue raised in this study was that US contracting officers do not always recognize this exemption, which becomes a source of friction. The reality is these MoUs do not exempt potential NTIB suppliers from all US domestic-source restrictions—most notably, restrictions in the Berry Amendment (section 2533a of title 10, United States Code) for textiles and a similar restriction on specialty metals (section 2533b of title 10, United States Code). One interviewee proposed that the NTIB become part of the Berry Amendment and specialty-metals coverage:

> "To provide the basis for already commonly applied 'Domestic Non-Availability Determinations' to be deemed unnecessary within the NTIB, as sourcing textiles and speciality metals, for instance, should be feasible from anywhere within the NTIB. This approach would remove a level of bureaucracy that otherwise has to be overcome to ultimately allow a transaction to go ahead, which adds cost for little benefit. In addition, considering the entire NTIB when sourcing such materials could afford greater security of supply of the manufactured goods affected."

This would require amending the Berry Amendment and expanding the coverage to the NTIB from the United States. But, because textile production in the United States and the Berry Amendment are a particularly politically charged issue in the United States, it is unlikely to be changed significantly in the near term. Still, it makes little sense that an NTIB nation should be forced to comply with the bureaucracy involved with Berry—particularly the compliance requirement on *de minimis* amounts of fiber in a technology made outside the United States. As such, it would be advantageous to obtain a Berry *de minimis* standard for end items produced by NTIB countries and exported to the United States. This would have no impact on US textile production, as the fabric would be in trifling amounts incorporated into an end-item defense product produced in an NTIB country. At the same time, to maintain the goals of the Berry Amendment, any such relief to the NTIB countries could not apply to textile end items.

Legislative Proposal 3B

Treatment of Products Produced in National Technology Industrial Base under Berry Amendment

(a) In General.—Section 2533a (d) of title 10, United States Code, is amended by inserting after (d)(4), the following—

(5) A minimum threshold that is *de miminus* to a larger end item supplied by a country that is part of the national technology industrial base, as defined in section 2500 of title 10, United States Code.

Any issues within the NTIB related to the implementation of the specialty-metals domestic-source restriction found in section 2533b of title 10, United States Code should be able to be addressed by the Quadrilateral Council using the authority found in subsection (d) of 2533b, which addresses an exception relating to agreements with foreign governments. If necessary, any such agreement could be negotiated under that authority among the NTIB countries if the specialty-metals language is found to hinder defense cooperation and the seamless integration of the NTIB.

==========

Recommendation #4: NTIB industrial-base approaches should serve as a test bed for innovations in international cooperation and be applied on a case-by-case basis to other close allies, and to further civil-military integration between Silicon Valley and the Department of Defense.

The NTIB can be the emerging test bed for innovation in international cooperation and civil-military integration. While there are many distinct, historical cooperative aspects of the United States' relationship with Canada, Australia, and the UK, a similar argument exists as to whether to conduct greater industrial cooperation with other close allies. The reality is that the culture of the bureaucracy managing the technological-transfer process is probably not yet ready to embrace any such expansion beyond the NTIB countries, until it accepts the implications of a new great-power threat environment. Even addressing only the NTIB will meet stiff resistance from those still stuck in a 1970s mindset.

In the meantime, the NTIB can provide an analytical framework for future defense-cooperation and

industrial-integration efforts between the United States and other close allies. Measures can be tested within the NTIB and, where possible, expanded to the next tier of close allies, either in whole or in part. In some of these countries, the United States may only be interested in one or two capabilities that exist in a handful of firms. The trusted community could be expanded, and a best-practice criteria of control measures could be applied to just those firms, and within portions of other allied governments.

The potential US approach for international cooperation with its allies could be based on the following model. While the United States has relationships with many countries, its closest allies have established Reciprocal Defense Procurement and Acquisition Policy Memoranda of Understanding with the United States on defense cooperation. Currently, the following twenty-seven countries have such an MoU.

Australia

Austria

Belgium

Canada

Czech Republic

Denmark

Egypt

Estonia

Finland

France

Germany

Greece

Israel

Italy

Japan

Latvia

Luxembourg

Netherlands

Norway

Poland

Portugal

Slovenia

Spain

Sweden

Switzerland

Turkey

United Kingdom

This is the entry point to the establishment of greater industrial-base cooperation and integration. The next level of integration—and what will be proposed as potential candidates for greater cooperation—would be those countries that have a security-of-supply agreement with the United States. A security-of-supply arrangement is a key criterion for cooperation, as these countries have agreed to mechanisms similar to the Defense Priorities and Allocation System under the US Defense Production Act of 1950 (P.L. 81-774, 50 U.S.C. §§4501 et seq.). This commits these countries to supply the US military, on a reciprocal basis, ahead of their own civilian and defense needs. These types of arrangements proved extremely useful during the Iraq conflict for the production of mine-resistant ambush protected vehicles (MRAPs) and counter-IED equipment. Currently, the following six countries in addition to the UK, Canada, and Australia have such a security-of-supply agreement.

Finland

Italy

Norway

Netherlands

Spain

Sweden

Some of these security-of-supply nations could become the next eligible entrants into either the NTIB or an NTIB-light mechanism that would allow for an "a la carte" menu of cooperative measures to be pursued with these nations. Thus, a next tier of close allies could be brought into any of the industrial-policy regimes, such as those established and tested within the NTIB to coordinate foreign investment, security of supply chain, and technology transfer, either in full or in part. The United States could also consider doing this for some applications on a multilateral basis within NATO, and bilaterally with other non-NATO allies.

To encourage this type of approach, Congress could consider the following legislation.

Legislative Proposal 4A:

ADOPTION OF NATIONAL TECHNOLOGY INDUSTRIAL BASE STREAMLINING AND HARMONIZATION POLICIES AND PROCEDURES

(a) In General.—The Chairman of the National Defense Technology and Industrial Base Council as defined by section 2502 of title 10, United States Code, shall—

> **(1) periodically review whether any industrial base streamlining or harmonization policy or regulation related to industrial security and security**

of supply chain, cybersecurity, regulating foreign direct investment and foreign ownership, control, and influence mitigation; market research, technology assessment and research cooperation within public and private research-and-development organizations and universities, technology and export-control measures, acquisition processes and oversight, and management best practices that applies to the national technology industrial base as defined in section 2500(1) of title 10, United States Code, should apply in full or in part to specified countries who have reciprocal defense security of supply agreements with the United States; and

(2) incorporate any such changes in a modified bilateral reciprocal defense agreement with the United States.

==========

As US allies are eventually tiered for industrial-cooperation purposes into MoU, security-of-supply, and NTIB-lite countries, the US government may wish to expand the original NTIB in the future. Additional criteria—such as the closeness of the intelligence, missile defense, or a nuclear-weapons cooperative relationship—may be considerations for future granting of NTIB benefits. In 2016, the Senate Armed Services Committee briefly considered harmonizing the NTIB with the so-called "Five Eyes" intelligence alliance. Unfortunately, little was known in the committee about New Zealand's defense-industrial base at the time and, because legislation was moving quickly, New Zealand was left out of the NTIB. New Zealand has a complementary industrial base, and could be considered for NTIB status after a few years' time. While New Zealand has an MoU with the United States, it does not have a security-of-supply arrangement in place. However, it is advisable that such an agreement should be negotiated and operative before New Zealand is added to the NTIB, despite its "Five Eyes" qualifications. To incentivize such an agreement, Congress may want to consider the following.

Legislative Proposal 4B:

AMENDMENT TO DEFINITION OF NATIONAL TECHNOLOGY AND INDUSTRIAL BASE.

(a) In General.—Upon the determination of the Secretary of Defense that it is in the U.S. national security interest, and after the successful negotiation and operation of a reciprocal security-of-supply agreement between the United States and New Zealand, 30 days after such determination is made, Section 2500(1) of title 10, United States Code, is amended by inserting", New Zealand," after Australia.

==========

In addition, a process for adding other members to the NTIB could be established. This process would incentivize greater cooperation between the United States and its allies and while much harmonization could come through providing benefits through an *a la carte* menu of cooperative measures in a NTIB-lite arrangement, it may be in the US interest to add additional partners to the NTIB in the coming decade.

Legislative Proposal 4C:

ADDITIONAL MEMBERS OF THE NATIONAL TECHNOLOGY INDUSTRIAL BASE.

(a) In General.—The Chairman of the National Defense Technology and Industrial Base Council as defined by section 2502 of title 10, United States Code, shall periodically review the list of countries who have reciprocal defense agreements with the United States to determine if of those any countries should be added to the National Technology Industrial Base.

(b) Frequency of Review.—The review required by subsection (a) shall, at a minimum, be conducted every five years.

(c) Report Required.—Not later than 260 days after the date of enactment of this Act, the Chairman of the National Defense Technology and Industrial Base Council shall submit a report to the congressional defense committees a report containing the results of the review required by subsection (a).

==========

Finally, Silicon Valley faces the same extraterritoriality and ITAR taint technology-transfer barriers that confront the US closest allies. Without changes to the export-control system, the US military will deprive itself of commercial advances in technology that will then become widely available to adversaries. Thus, the national technology-industrial base can serve as a test bed for greater cooperation with not only close allies, but with the types of companies represented in Silicon Valley writ large, to bring together the scientific and engineering elite residing in the United States and its allies, to address defense-technology needs.

Until ITAR and export controls are reformed, they will become the most significant barriers to greater DoD-Silicon Valley cooperative efforts in the future. If the United States cannot first agree on a new construct with its closest allies, it is doubtful it will be able to remove the barriers to achieving greater civil-military integration with global commercial companies in the United States, which can move their research outside of the United States fairly quickly if export controls were applied to AI, data analytics, autonomous systems, and others, as recent rule making has suggested.[45]

If the United States attempts to overcontrol emerging commercial technologies, it could take advantage, through a reformed NTIB, of the potential regulatory arbitrage that Silicon Valley firms would induce by moving their research and development to Canada, Australia, or the UK. Under such a scenario, the United States could access Silicon Valley through its allies. Ideally, however, it is better to design an export-control process that integrates Silicon Valley into a civil-militarily integrated NTIB, as envisioned in section 2501(b) of title 10, United States Code. The following proposal would attempt to focus the United States on that policy goal.

Legislative Proposal 4D:

CIVIL-MILITARY INTEGRATION ENHANCEMENT MEASURES.

(a) In General.—The Chairman of the National Defense Technology and Industrial Base Council, as defined by section 2502 of title 10, United States Code, shall review the impact of the International Traffic in Arms Regulations on the ability of the U.S. government to jointly conduct research and development and acquire solutions from leading non-traditional contractors as defined in 2302(9) of title 10, United States Code.

(b) Required Elements.—Such a review shall include the impact of limitations placed on nontraditional contractors through the acceptance of defense fund, and the extraterritorial limitations placed on nontraditional contractors that limit the goal of civil-military integration of the defense industrial base, as required under section 2501(b) of title 10, United States Code.

(c) Report Required.—Not later than 260 days after the date of enactment of this Act, the Chairman of the National Defense Technology and Industrial Base Council shall submit a report to the congressional defense committees a report summarizing the results of the review required by subsection (a).

==========

45 Footnote on emerging tech rule

CONCLUSION

This project identified and assessed: the barriers to the US statutory requirement for the "seamless integration of the persons and organizations" within the industrial bases of the four countries that comprise the NTIB; and the specific legal, regulatory, and policy changes needed to achieve such integration. Despite the closeness of the intelligence and military relationships between the NTIB countries, it has become increasingly difficult to work together on disruptive innovation, and to transfer military technology between these countries.

This is primarily due to a US export-control system that was designed for a place in time when the United States maintained a technological dominance that no longer exists. The result is the US technology-control apparatus now promotes US technological inferiority, by primarily controlling technology widely available to great-power adversaries, while disincentivizing research-and-development cooperation with allies and the commercial market. Many of the so-called second offset military technologies, which were the source of US technological dominance for decades, have long since proliferated to adversaries. Technological superiority is now being established beyond the reaches of the US government, not least of all in a globalized, commercial industry, where firms face many of the same barriers to greater defense cooperation with the DoD that allies do.

As US technological dominance weakens, there is a compelling case to be made to establish greater momentum in NTIB integration. The growing threat facing the United States cannot be met on its own. If the United States cannot step up and design a way to integrate the defense and commercial industrial capabilities of both it and its allies—that supports both technological and economic dominance—it will likely lose a future conflict. The stakes are that high. To merely compete with countries such as China, which already has a population much larger than the United States' and will eventually have a larger economy, will require allies. The United States needs to work with these allies, leveraging the technical expertise resident in their countries and in the commercial market.

If the United States cannot develop a harmonized industrial strategy and a technology control-system that works with the UK, Australia, and Canada, it has no hope of doing so with its other allies—or, for that matter, with globalized commercial companies in Silicon Valley, Boston's technology corridor, or Austin. An autarkic, go-it-alone strategy will eventual leave the United States to compete on its own against a civilly-military integrated China, as allies and the commercial marketplace hold back better technology out of fear of getting entangled in the US export-control system. Meanwhile, China will be doing its best to buy, steal, and replicate this technology, and to incorporate it into its own military systems. This is not a winning strategy.

The proposals outlined in this study should not be seen as the last word on what needs to be done, but as a mechanism to initiate action and debate on closing the technology gap by expanding the industrial base. At the same time, to merely tinker around the edges with what has worked in the past, rather than think boldly, is a recipe for failure.

A clear vision is needed for a "free-trade area" in technologies relevant, or potentially relevant, to national security, underpinned by broadly expansive exemptions for controls within the NTIB countries. This would address the ITAR taint and extraterritoriality issues, and operate within a trusted community of cleared entities. It would be a first step toward reestablishing US and allied technological dominance. The next step is to advance lessons learned from the NTIB experience, to establish closer cooperation with Silicon Valley and the next tier of closest US allies. The current technology-control process is now counterproductive to meeting national security needs, and requires a massive overhaul. The NTIB allows for the opportunity to get those changes right by testing policy alternatives within a trusted community.

While many of the proposals outlined in this study could be implemented through the regulatory process by administrative fiat, that they weren't in the past implies that the executive branch has not come to terms with the severity of the threat and the loss of US technological superiority. Congress may need to act, as the DoD and the Department of State have yet been incapable of acting with any sense of resolve. It would be best if the administration acted immediately under its current authority, but this authority has historically been delegated many levels down in the bureaucracy, and the regulatory process often resorts to a system of least-common-denominator, incremental actions. This is the result of the give and take within the interagency process that has played out on technology-transfer issues over the past decades.

Still, the politics on the Hill may be no better than in the administration, and much will depend on congressional support. Political change in the next few years will pivot on whether the changing threat environment and the loss of technology leadership are enough to modify attitudes and longstanding views held in important parts of both the administration and Congress. It is vital for Congress and the administration to understand current technology trends, where the United States is falling behind, and where it needs to incentivize cooperation with its allies and the commercial marketplace. The place to start is in the trusted space of the NTIB. These are the countries and militaries that have stood shoulder to shoulder with the United States for the last century. There is little reason to try controlling their foreign and defense policies through extraterritorial application of the ITAR. There does not need to be an assumption that, because the United States contributed in some way to the research and development of a new idea, it gets to control all uses of anything that might ultimately derive from that participation. Close allies can be trusted to use this technology to defend themselves and support the United States when needed, and the United States can do the same.

Appendices

Appendix A: National Technology Industrial Base in US Law (Title 10, United States Code)

10 U.S. Code § 2500—Definitions

In this chapter:

(1) The term "national technology and industrial base" means the persons and organizations that are engaged in research, development, production, integration, services, or information technology activities conducted within the United States, the United Kingdom of Great Britain and Northern Ireland, Australia, and Canada.

10 U.S. Code § 2501—National Security Strategy for National Technology and Industrial Base

(a) **National Security Strategy for National Technology and Industrial Base.—**The Secretary of Defense shall develop a national security strategy for the national technology and industrial base. Such strategy shall be based on a prioritized assessment of risks and challenges to the defense supply chain and shall ensure that the national technology and industrial base is capable of achieving the following national security objectives:

(1) Supplying, equipping, and supporting the force structure of the armed forces that is necessary to achieve—

(A) the objectives set forth in the national security strategy report submitted to Congress by the President pursuant to section 108 of the National Security Act of 1947 (50 U.S.C. 3043);

(B) the policy guidance of the Secretary of Defense provided pursuant to section 113(g) of this title; and

(C) the future-years defense program submitted to Congress by the Secretary of Defense pursuant to section 221 of this title.

(2) Sustaining production, maintenance, repair, logistics, and other activities in support of military operations of various durations and intensity.

(3) Maintaining advanced research and development activities to provide the armed forces with systems capable of ensuring technological superiority over potential adversaries.

(4) Reconstituting within a reasonable period the capability to develop, produce, and support supplies and equipment, including technologically advanced systems, in sufficient quantities to prepare fully for a war, national emergency, or mobilization of the armed forces before the commencement of that war, national emergency, or mobilization.

(5) Providing for the development, manufacture, and supply of items and technologies critical to the production and sustainment of advanced military weapon systems within the national technology and industrial base.

(6) Providing for the generation of services capabilities that are not core functions of the armed forces and that are critical to military operations within the national technology and industrial base.

(7) Providing for the development, production, and integration of information technology within the national technology and industrial base.

(8) Maintaining critical design skills to ensure that the armed forces are provided with systems capable of ensuring technological superiority over potential adversaries.

(9) Ensuring reliable sources of materials that are critical to national security, such as specialty metals, essential minerals, armor plate, and rare earth elements.

(10) Reducing, to the maximum extent practicable, the presence of counterfeit parts in the supply chain and the risk associated with such parts.

(b) **Civil-Military Integration Policy.—** The Secretary of Defense shall ensure that the United States attains the national technology and industrial base objectives set forth in subsection (a) through acquisition policy reforms that have the following objectives:

(1) Relying, to the maximum extent practicable, upon the commercial national technology and industrial base that is required to meet the national security needs of the United States.

(2) Reducing the reliance of the Department of Defense on technology and industrial base sectors that are economically dependent on Department of Defense business.

(3) Reducing Federal Government barriers to the use of commercial products, processes, and standards.

10 U.S. Code § 2502—National Defense Technology and Industrial Base Council

(a) **Establishment.—** There is a National Defense Technology and Industrial Base Council.

(b) **Composition.—** The Council is composed of the following members:

(1) The Secretary of Defense, who shall serve as chairman.

(2) The Secretary of Energy.

(3) The Secretary of Commerce.

(4) The Secretary of Labor.

(5) Such other officials as may be determined by the President.

(c) **Responsibilities.—** The Council shall have the responsibility to ensure effective cooperation among departments and agencies of the Federal Government, and to provide advice and recommendations to the President, the Secretary of Defense, the Secretary of Energy, the Secretary of Commerce, and the Secretary of Labor, concerning—

(1) the capabilities of the national technology and industrial base to meet the national security objectives set forth in section 2501(a) of this title;

(2) programs for achieving such national security objectives; and

(3) changes in acquisition policy that strengthen the national technology and industrial base.

(d) **Alternative Performance of Responsibilities.—** Notwithstanding subsection (c), the President may assign the responsibilities of the Council to another interagency organization of the executive branch that includes among its members the officials specified in paragraphs (1) through (4) of subsection (b).

10 U.S. Code § 2503—National Defense Program for Analysis of the Technology and Industrial Base

(a) **Establishment.—** The Secretary of Defense shall establish a program for analysis of the national technology and industrial base.

(b) **Supervision of Program.—** The Secretary of Defense shall carry out the program through the Under Secretary of Defense for Acquisition, Technology, and Logistics. In carrying out the program, the Under Secretary shall consult with the Secretary of Energy, the Secretary of Commerce, and the Secretary of Labor.

(c) **Functions—** The functions of the program shall include, with respect to the national technology and industrial base, the following:

(1) The assembly of timely and authoritative information.

(2) Initiation of studies and analyses.

(3) Provision of technical support and assistance to—

(A) the Secretary of Defense for the preparation of the periodic assessments required by section 2505 of this title;

(B) the defense acquisition university structure and its elements; and

(C) other departments and agencies of the Federal Government in accordance with guidance established by the Council.

(4) Dissemination, through the National Technical Information Service of the Department of Commerce, of unclassified information and assessments for further dissemination within the Federal Government and to the private sector.

10 U.S. Code § 2504—Annual Report to Congress

The Secretary of Defense shall transmit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives by March 1 of each year a report which shall include the following information:

(1) A description of the departmental guidance prepared pursuant to section 2506 of this title.

(2) A description of the assessments prepared pursuant to section 2505 of this title and other analyses used in developing the budget submission of the Department of Defense for the next fiscal year.

(3) Based on the strategy required by section 2501 of this title and on the assessments prepared pursuant to section 2505 of this title—

(A) a description of any mitigation strategies necessary to address any gaps or vulnerabilities in the national technology and industrial base; and

(B) any other steps necessary to foster and safeguard the national technology and industrial base.

(4) Identification of each program designed to sustain specific essential technological and industrial capabilities and processes of the national technology and industrial base.

10 U.S. Code § 2505—National technology and industrial base: periodic defense capability assessments

(a) **Periodic Assessment.—** Each fiscal year, the Secretary of Defense shall prepare selected assessments of the capability of the national technology and industrial base to attain the national security objectives set forth in section 2501(a) of this title. The Secretary of Defense shall prepare such assessments in consultation with the Secretary of Commerce and the Secretary of Energy.

(b) **Assessment Process.—** The Secretary of Defense shall ensure that technology and industrial capability assessments—

(1) describe sectors or capabilities, their underlying infrastructure and processes;

(2) analyze present and projected financial performance of industries supporting the sectors or capabilities in the assessment;

(3) determine the extent to which the requirements associated with defense acquisition programs can be satisfied by the present and projected performance capacities of industries supporting the sectors or capabilities in the assessment, evaluate the reasons for any variance from applicable preceding determinations, and identify the extent to which those industries are comprised of only one potential source in the national technology and industrial base or have multiple potential sources;

(4) determine the extent to which the requirements associated with defense acquisition programs can be satisfied by the present and projected performance capacities of industries that do not actively support Department of Defense acquisition programs and identify the barriers to the participation of those industries;

(5) identify technological and industrial capabilities and processes for which there is potential for the national industrial and technology base not to be able to support the achievement of national security objectives; and

(6) consider the effects of the termination of major defense acquisition programs (as the term is defined in section 2430 of this title) or major automated information system programs (as defined in section 2445a [1] of this title) in the previous fiscal year on the sectors and capabilities in the assessment.

(c) Assessment of Extent of Dependency on Foreign Source Items.—Each assessment under subsection (a) shall include a separate discussion and presentation regarding the extent to which the national technology and industrial base is dependent on items for which the source of supply, manufacture, or technology is outside of the United States and Canada and for which there is no immediately available source in the United States or Canada. The discussion and presentation regarding foreign dependency shall—

(1) identify cases that pose an unacceptable risk of foreign dependency, as determined by the Secretary; and

(2) present actions being taken or proposed to be taken to remedy the risk posed by the cases identified under paragraph (1), including efforts to develop a domestic source for the item in question.

(d) Assessment of Extent of Effects of Foreign Boycotts.—Each assessment under subsection (a) shall include an examination of the extent to which the national technology and industrial base is affected by foreign boycotts. If it is determined that a foreign boycott (other than a boycott addressed in a previous assessment) is subjecting the national technology and industrial base to significant harm, the assessment shall include a separate discussion and presentation regarding that foreign boycott that shall, at a minimum—

(1) identify the sectors that are subject to such harm;

(2) describe the harm resulting from such boycott; and

(3) identify actions necessary to minimize the effects of such boycott on the national technology and industrial base.

(e) **Integrated Process.—** The Secretary of Defense shall ensure that consideration of the technology and industrial base assessments is integrated into the overall budget, acquisition, and logistics support decision processes of the Department of Defense.

10 U.S. Code § 2506—Department of Defense technology and industrial base policy guidance

(a) **Departmental Guidance.—** The Secretary of Defense shall prescribe departmental guidance for the attainment of each of the national security objectives set forth in section 2501(a) of this title.

(b) **Purpose of Guidance.—** The guidance prescribed pursuant to subsection (a) shall provide for technological and industrial capability considerations to be integrated into the strategy, management, budget allocation, acquisition, and logistics support decision processes.

Appendix B: Section 881 of the National Defense Authorization Act for Fiscal Year 2017 and subsequent NTIB provisions enacted in the 2018 and 2019 NDAAs

SEC. 881. Greater Integration Of The National Technology And Industrial Base.

(a) PLAN REQUIRED.—Not later than January 1, 2018, the Secretary of Defense shall develop a plan to reduce the barriers to the seamless integration between the persons and organizations that comprise the national technology and industrial base (as defined in section 2500 of title 10, United States Code). The plan shall include at a minimum the following elements:

(1) A description of the various components of the national technology and industrial base, including government entities, universities, nonprofit research entities, nontraditional and commercial item contractors, and private contractors that conduct commercial and military research, produce commercial items that could be used by the Department of Defense, and produce items designated and controlled under section 38 of the Arms Export Control Act (also known as the ''United States Munitions List'').

(2) Identification of the barriers to the seamless integration of the transfer of knowledge, goods, and services among the persons and organizations of the national technology and industrial base.

(3) Identification of current authorities that could contribute to further integration of the persons and organizations of the national technology and industrial base, and a plan to maximize the use of those authorities.

(4) Identification of changes in export control rules, procedures, and laws that would enhance the civil-military integration policy objectives set forth in section 2501(b) of title 10, United States Code, for the national technology and industrial base to increase the access of the Armed Forces to commercial products, services, and research and create incentives necessary for nontraditional and commercial item contractors, universities, and nonprofit research entities to modify commercial products or services to meet Department of Defense requirements.

(5) Recommendations for increasing integration of the national technology and industrial base that supplies defense articles to the Armed Forces and enhancing allied interoperability of forces through changes to the text or the implementation of—

(A) section 126.5 of title 22, Code of Federal Regulations (relating to exemptions that are applicable to Canada under the International Traffic in Arms Regulations);

(B) the Treaty Between the Government of the United States of America and the Government of Australia Concerning Defense Trade Cooperation, done at Sydney on September 5, 2007;

(C) the Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defense Trade Cooperation, done at Washington and London on June 21 and 26, 2007; and

(D) any other agreements among the countries comprising the national technology and industrial base.

(b) AMENDMENT TO DEFINITION OF NATIONAL TECHNOLOGY AND INDUSTRIAL BASE.—Section 2500(1) of title 10, United States Code, is amended by inserting '', the United Kingdom of Great Britain and Northern Ireland, Australia,'' after ''United States''.

(c) REPORTING REQUIREMENT.—The Secretary of Defense shall report on the progress of implementing the plan in subsection (a) in the report required under section 2504 of title 10, United States Code.

SEC. 808. Defense Policy Advisory Committee On Technology.

(a) **ESTABLISHMENT.—** Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, acting through the Chief Management Officer, shall form a committee of senior executives from United States firms in the national technology and industrial base to meet with the Secretary, the Secretaries of the military departments, and members of the Joint Chiefs of Staff to exchange information, including, as appropriate, classified information, on technology threats to the national security of the United States and on the emerging technologies from the national technology and industrial base that may become available to counter such threats in a timely manner.

(b) MEETINGS.—The defense policy advisory committee on technology formed pursuant to subsection (a) shall meet with the Secretary and the other Department of Defense officials specified in such subsection collectively at least once annually in each of fiscal years 2018 through 2022. The Secretary of Defense shall provide the congressional defense committees annual briefings on the meetings.

(c) FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the defense policy advisory committee on technology established pursuant to this section.

SEC. 1712. Review Regarding Applicability Of Foreign Ownership, Control, Or Influence Requirements Of National Industrial Security Program To National Technology And Industrial Base Companies.

(a) REVIEW.—The Secretary of Defense, with the concurrence of the Secretary of State and after consultation with the Director of the Information Security Oversight Office, shall review whether organizations whose ownership or majority control is based in a country that is part of the national technology and industrial base should be exempted from one or more of the foreign ownership, control, or influence requirements of the National Industrial Security Program.

(b) AUTHORITY.—The Secretary of Defense may establish a program to exempt organizations described under subsection (a) from one or more of the foreign ownership, control, or influence requirements of the National Industrial Security Program. Any such program shall comply with the requirements of this subsection.

(1) IN GENERAL.—Under a program established under this subsection, the Secretary, with the concurrence of the Secretary of State and after consultation with the Director of the Information Security Oversight Office, shall maintain a list of organizations owned or controlled by a country that is part of the national technology and industrial base that are eligible for exemption from the requirements described under such subsection.

(2) DETERMINATIONS OF ELIGIBILITY.—Under a program established under this subsection, the Secretary of Defense, with the concurrence of the Secretary of State and after consultation with the Director of the Information Security Oversight Office, may (on a case-by-case basis and for the purpose of supporting specific needs of the Department of Defense) designate an organization whose ownership or majority control is based in a country that is part of the national technology and industrial base as exempt from the requirements described under sub-section (a) upon a determination that such exemption—

(A) is beneficial to improving collaboration within countries that are a part of the national technology and industrial base;

(B) is in the national security interest of the United States; and

(C) will not result in a greater risk of the disclosure of classified or sensitive information consistent with the National Industrial Security Program.

(3) EXERCISE OF AUTHORITY.—The authority under this subsection may be exercised beginning on the date that is the later of—

(A) the date that is 60 days after the Secretary of Defense, in consultation with the Secretary of State and the Director of the Information Security Oversight Office, submits to the appropriate congressional committees a report summarizing the review conducted under subsection (a); and

(B) the date that is 30 days after the Secretary of Defense, in consultation with the Secretary of State and the Director of the Information Security Oversight Office, submits to the appropriate congressional committees a written notification of a determination made under paragraph (2), including a discussion of the issues related to the foreign ownership or control of the organization that were considered as part of the determination.

(c) DEFINITIONS.— In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' has the meaning given the term in section 301 of title 10, United States Code.

(2) NATIONAL TECHNOLOGY AND INDUSTRIAL BASE.—the term ''national technology and industrial base'' has the meaning given the term in section 2500 of title 10, United States Code.

SEC. 845. Report On Defense Electronics Industrial Base.

(a) IN GENERAL.—Not later than January 31, 2019, the Secretary of Defense, in consultation with the Executive Agent for Printed Circuit Board and Interconnect Technology and the Director of the Office of Management and Budget, shall submit to Congress a report examining the health of the defense electronics industrial base, including analog and passive electronic parts, substrates, printed boards, assemblies, connectors, cabling, and related areas, both domestically and within the national technology and industrial base.

(b) ELEMENTS.—The report required under subsection (a) shall include the following elements:

(1) An examination of current and planned partnerships with the commercial industry.

(2) Analysis of the current and future defense electronics industrial base.

(3) Threat assessment related to system security.

(4) An assessment of the health of the engineering and production workforce.

(5) A description of the electronics supply chain requirements of defense systems integral to meeting the goals of the 2018 National Defense Strategy.

(6) Recommended actions to address areas deemed deficient or vulnerable, and a plan to formalize long-term resourcing for the Executive Agent.

(7) Any other areas matters determined relevant by the Secretary.

SEC. 842. Removal Of National Interest Determination Requirements For Certain Entities.

(a) IN GENERAL.—Effective October 1, 2020, a covered NTIB entity operating under a special security agreement pursuant to the National Industrial Security Program shall not be required to obtain a national interest determination as a condition for access to proscribed information.

(b) ACCELERATION AUTHORIZED.—Notwithstanding the effective date of this section, the Secretary of Defense, in consultation with the Director of the Information Security Oversight Office, may waive the requirement to obtain a national interest determination for a covered NTIB entity operating under such a special security agreement that has—

(1) a demonstrated successful record of compliance with the National Industrial Security Program; and

(2) previously been approved for access to proscribed information.

(c) DEFINITIONS.— In this section:

(1) COVERED NTIB ENTITY.—The term ‘‘covered NTIB entity’’ means a person that is a subsidiary located in the United States—

(A) for which the ultimate parent company and any intermediate parent companies of such subsidiary are located in a country that is part of the national technology and industrial base (as defined in section 2500 of title 10, United States Code); and

(B) that is subject to the foreign ownership, control, or influence requirements of the National Industrial Security Program.

(2) PROSCRIBED INFORMATION.—The term ‘‘proscribed information’’ means information that is—

(A) classified at the level of top secret;

(B) communications security information (excluding controlled cryptographic items when un-keyed or utilized with unclassified keys);

(C) restricted data (as defined in section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014));

(D) special access program information under section 4.3 of Executive Order No. 13526 (75 Fed. Reg. 707; 50 U.S.C. 3161 note) or successor order; or

(E) designated as sensitive compartmented information.

About the Author

Bill Greenwalt is a nonresident senior fellow at the Atlantic Council within the Scowcroft Center for Strategy and Security, and specializes in industrial-base and defense-management reform issues. Previously, Mr. Greenwalt worked as a professional staff member on the US Senate Armed Services Committee, responsible for legislative reform efforts in the Pentagon. Prior to that, he served in senior positions at the Pentagon, where he was deputy undersecretary of defense for industrial policy, and in Congress in both the Senate and House of Representatives, and in the defense industry. He is also currently an advisor, board member, and consultant to a range of government, nonprofit, and private-sector entities on defense and government matters.

Acknowledgments

This report is the culmination of a reseach project, "Implementing the National Technology Industrial Base," which has been directed by Senior Fellow Steven Grundman and overseen by Barry Pavel, Senior Vice President and Director of the Scowcroft Center for Strategy and Security. It is made possible in part through the generous support of Safran, MBDA, and Innovation Norway, whose representatives served on the project's steering committee, as well as the Norwegian-American Defense and Homeland Security Industry Council and its member companies Kongsberg and NAMMO.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org