Securing the United States Defense ICT Supply Chain of the Future

> The perception [...] is that DoD's current supply chain exists to build the military we have."[1]

1. "Report of the Defense Critical Supply Chain Task Force," House Armed Services Committee, Jul. 22, 2021, p. 13. https://web.archive.org/web/20220712210401/https://armedservices.house.gov/_cache/files/e/5/e5b9a98f-9923-47f6-a5b5-ccf77ebbb441/7E26814EA08F7F701B16D4C5FA37F043.defense-critical-supply-chain-task-force-report.pdf.

Table of Contents

Executive Summary

The defense information and communications technology (ICT) supply chain is integral to U.S. security and competitiveness on the world stage. As recent reports, such as the 2023 National Cybersecurity Strategy and the Annual Threat Assessment of the U.S. Intelligence Community have affirmed, the ICT supply chain continues to face risks that were only exacerbated by the COVID-19 pandemic, the rise of decoupling, the increasing threat of power conflicts, and the new challenges and opportunities presented by emerging technologies. These issues, among others, have created an operational environment in which current approaches to assuring military readiness are unsatisfactory.

Current attempts to remediate the problem have been heavily focused on immediate and short-term solutions, but a longer-term, strategic view is necessary to ensure that the United States can defend itself moving forward. In an attempt to address these concerns from a broader perspective, the R Street Institute (RSI) convened a working group composed of leaders in cybersecurity, the armed forces, and the intelligence community to refine recommendations and a strategy for the future. This paper details the findings and recommendations compiled by the working group after a year of collaborative engagement.

Disclaimer:

The views presented in this policy paper are the views of the authors and working group members, and do not necessarily represent the view of R Street Institute, the Department of Defense or any affiliations they retain.

Introduction

Over the past several years, it has become increasingly clear that many of the United States' defense-critical supply chains are dangerously vulnerable. Of the varied processes and products that power the national security industrial base, the information and communications technology (ICT) supply chain is particularly at risk.

Part of this vulnerability is inherent. The defense ICT supply chain is complex and dynamic and relies on entities and processes beyond the scope of the United States in general, the U.S. government or defense sector control. A functioning and robust supply chain not only needs to guarantee sufficient and continued access to critical products, services and technologies, but also to ensure their integrity from a quality and security perspective. This is a difficult prospect in an era in which control over key elements of the ICT supply chain has been lost, increasingly complex software continues to evolve, and novel technological innovations challenge assumptions of security.

Nevertheless, these vulnerabilities must be identified and mitigated to the maximum extent feasible, in the near-, mid- and far-terms. The disruptions of the COVID-19 pandemic, the rise of China as a near-peer competitor, the ongoing Russo-Ukrainian War and the rapid evolution of new technologies have forced the realization that the status quo is not acceptable.

To address these problems, a number of expert boards and task forces have convened to study the existing environment, define and scope the supply-chain problem, and present solutions.[2] The outcomes of these efforts, many of which are available for reference in Appendix A, offer hundreds of pages of insights into the depth of the security problems that currently confront the defense sector. They reveal several challenges for the United States, which are summarized in a literature review in a later section.

Efforts to recognize and address current challenges are important, but ultimately fall short of what is needed to truly remediate existing vulnerabilities and, of greater importance, prevent future ones. In an environment defined by change, the United States must take a forward-leaning approach and formulate a strategy that drives the right policies, processes, and resourcing to anticipate and address likely future threats. In other words, it requires a strategy that is proactive rather than reactive. The need for a future strategic approach is the focus of this paper.

2. See Appendix A.

Introduction

Without such an approach, we may fall further behind in key areas. We also risk tooling the supply chain to meet present challenges, rather than optimizing it to anticipate and mitigate future risks. In focusing on remediating current vulnerabilities, we may overlook an entirely new set of challenges—particularly when considering that emerging developments in quantum computing, artificial intelligence, state of the art microelectronics manufacturing and other advances in technology will alter our current understanding of the threat landscape. In short, we need a strategy to secure the defense ICT supply chain of the future, while mitigating as much risk as possible in the near- and mid-term while that future state is crafted. We need a multi-pronged framework that aggressively addresses known strategic areas of risk, and also anticipates and solves for other areas that will become critical before they become such.

This call for a future-focused, multi-pronged strategy is what distinguishes this paper from the existing body of literature on the defense sector and the supply chain. So, too, does our focus on a key aspect of broader supply-chain vulnerabilities: defense ICT. This paper itself is not a strategy but rather a call for a strategy. It is a call to those in a position to influence and affect change to look over the horizon and develop a strategy that orients and integrates all instruments of U.S. national power in a way that fundamentally reshapes how we architect and manage the defense ICT supply chain.

We begin by defining the defense ICT supply chain and describing the current landscape as identified by various task forces and reports. Then, we articulate assumptions for the future and desired end state. Next, we suggest guidelines for devising a future-oriented strategy, offering an initial set of principles to start the process. We conclude with a discussion of immediate next steps.

I. Defining the Defense ICT Supply Chain

In its broadest sense, the defense ICT supply chain is the sum total of the products, services and processes required to power the military and defense sectors and their industrial base in all ways that incorporate an element of information technology or digital communications.

For ease of reference and conceptualization, we divide the defense ICT supply chain into four components, which may overlap:

1. **Department of Defense-procured ICT**

   Such as software, hardware and managed IT services. These are the products and services the Department of Defense relies on for command, control, communications, computing, cyber, intelligence, surveillance, reconnaissance and targeting (C5ISRT) systems; and information operations functions and their security.

2. **ICT-specific components of platforms and capabilities**

   Such as weapons, vehicles and logistics systems. These are the digital components of the supply chain's weapons, weapons systems and power projection capabilities.

3. **ICT-specific elements of non-defense infrastructure and non-defense critical infrastructure, used by the Department of Defense (DoD) to perform its mission**

   Such as power grids, transportation networks, port security and more.

4. **The ICT-enabling fundamental building blocks and capabilities**

   Such as microelectronics (e.g. logic devices, memory devices, advanced analog to digital devices, etc.) and the assembly, packaging and testing of these components that provides the underpinning fabric of all ICT in the United States and the DoD.

While differing in a number of ways, these four layers of the defense ICT supply chain challenge share several key attributes. First, identifying and parsing the full scope of any of these components of the supply chain is difficult. Even non-defense supply chains are often opaque,

I. Defining the Defense ICT Supply Chain

complex and dynamic.[3] Adding a technological element only complicates the situation; consider, for example, the rapidly evolving nature of software. This knowledge deficit is only partly resolvable: as the report by the House Armed Services Committee (HASC) task force on the broader defense supply chain noted, "any static, 'comprehensive list' of priorities would be out of date almost immediately."[4] Nevertheless, an effective strategy to secure the supply chain demands a process that can identify and prioritize its key nodes and that remains up-to-date.

Second, while the defense ICT supply chain presents distinct challenges, its problems cannot be addressed in isolation. The defense supply chain not only relies on the direct products and services of the commercial sector, but also on the broader ecosystem that it facilitates. An example of the former is the military's reliance on civilian contractors to build fighter aircraft. An example of the latter includes things as simple as requiring toilet paper on base and depending on civilian shipping and transport, all of which contribute to a robust and diverse economy that enables economies of scale.

Third, while the efficient functioning of many supply chains is critical to American security, there are some elements that are more critical than others. We are speaking here of those elements of the defense ICT supply chain that undergird U.S. military readiness, power and force projection, and homeland security. Thus, while a toilet paper shortage may be frustrating, a shortage of critical microelectronics elements may be deadly.

Therefore, these four core elements of the defense ICT supply chain form the basis of our efforts in this paper. A strategy for the future of defense ICT supply chain security must address how to 1) appropriately scope of the challenge; 2) identify the elements that are within the control of the Defense Department and those that are not; and 3) determine, in a world of competing priorities, which products, processes, or capabilities are non-negotiable.

3. "Report of the Defense Critical Supply Chain Task Force," House Armed Services Committee, Jul. 22, 2021, pp. 9, 13. https://web.archive.org/web/20220712210401/https://armedservices.house.gov/_cache/files/e/5/e5b9a98f-9923-47f6-a5b5-ccf77ebbb441/7E26814EA08F7F701B16D4C5FA37F043.defense-critical-supply-chain-task-force-report.pdf.
4. Ibid.

II. Defense ICT Supply Chain Failures and Lessons Learned

A systematic review of the numerous in-depth reports on the state of the defense ICT supply chain (listed in Annex A) share a common theme: business-as-usual has not created the security outcomes necessary to ensure that the DoD can deliver on its mission. Moreover, they identify common areas in which there are deficiencies. Below, we briefly summarize and discuss the existing findings of past task force reports according to common themes across them.

A. Supply Chain Availability Risks

Perhaps the most obvious risk identified by prior supply chain task force reports is the insecurity of or uncertainty about the availability of critical products and raw materials—that is, the problem of supply chain disruptions or shortages. This could be due to natural disasters, adversarial actions, logistical problems, or because demand outstrips supply.

The issue of availability is exacerbated when manufacturing and materials acquisition and processing is concentrated heavily in certain geographic areas—especially where there is a foreign dependency—or when they rely heavily on special inputs.[5] In the case of geographic concentration, a disruption in supply can be caused by a natural disaster such as a pandemic, flood or other disaster (particularly those exacerbated by climate change), or simply by inefficient government policies. Perhaps more concerning is that an adversary could engineer a disruption or cutoff of supplies for strategic purposes. For example, the United States relies heavily on China to mine and process rare earth minerals: in the event of a crisis, it is possible that China could limit or cut off access to this supply. In the case of microelectronics, over 75 percent of all microelectronics used in ICT by the United States, including the DoD, comes from three countries: China, Taiwan and South Korea.[6] Any action that disrupts the availability of key components—especially for those which the United States no longer has the ability to produce itself—could be catastrophic. Recent efforts

5. See, e.g., "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," Department of Defense, September 2018, pp. 45-51. https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF; See, also "Fiscal Year 2020: Industrial Capabilities Report to Congress," Department of Defense OSD Industrial Policy, January 2021. https://media.defense.gov/2021/Jan/14/2002565311/-1/-1/0/FY20-INDUSTRIAL-CAPABILITIES-REPORT.PDF.
6. "Remarks by President Biden On Increasing the Supply of Semiconductors and Rebuilding Our Supply Chains," The White House, Jan. 21, 2022. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/01/21/remarks-by-president-biden-on-increasing-the-supply-of-semiconductors-and-rebuilding-our-supply-chains.

II. Defense ICT Supply Chain Failures and Lessons Learned

to bolster the microelectronics supply chain via the 2019 CHIPs for America Act and its funding, passed earlier this year, are important but insufficient, and have arrived too late to mitigate the obvious current problems.[7]

B. Supply Chain Integrity Risks

The second risk in supply chain management is that of integrity: Integrity is the assurance that existing products, materials, and services meet technical standards and specifications; are authentic (not counterfeit); and are designed and produced without "backdoors" or other defects subject to adversarial exploitation.[8] In short, we need deliberate efforts to increase the likelihood that ICT will work as expected at all times.

ICT adds an additional element to this challenge.[9] In the digital age, physical security to ensure product integrity is no longer enough. Ensuring the integrity of an analog device or piece of hardware may be difficult, but the challenges of ensuring the security of software are even greater. Further, it will be more challenging to integrate cutting edge technologies into existing and legacy systems, and to defend against their exploitation and attack.

C. Insufficient Planning, Policies and Processes

A related challenge is how government planning, process and policies shape the supply chain and contribute to its weaknesses.

Many of these insufficiencies are common to more than the supply chain challenge. One of the most recognizable is the perpetual problem of the "siloing" of information and inadequate information sharing among government agencies and between the government and private sector, which inhibits timely and effective policymaking and resource allocation.[10] Similarly, a lack of clarity about responsibility, accountability, authority

7. "H.R.4346 - 117th Congress (2021-2022): Chips and Science Act" Congress.gov, Library of Congress, 9 August 2022. https://www.congress.gov/bill/117th-congress/house-bill/4346.
8. See, e.g., "Supply Chain Security Strategy, Appendix 1 to DLA's 2018-2026 Strategic Plan," The Defense Logistics Agency, 2018, p. 2. https://www.dla.mil/Portals/104/Documents/Headquarters/StrategicPlan/SupplyChainSecurityStrategy.pdf.
9. See, e.g. "Securing Defense-Critical Supply Chains: An action plan developed in response to President Biden's Executive Order 14017," Department of Defense, February 2022, pp. 54-57. https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.
10. See, e.g. Chris Nissen et al., "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," MITRE, Aug. 3, 2018, p. ii. https://www.mitre.org/news-insights/publication/deliver-uncompromised-strategy-supply-chain-security-and-resilience.

II. Defense ICT Supply Chain Failures and Lessons Learned

and control of ICT supply-chain management across government agencies creates uncertainties about whose "problem" a given issue is—who oversees identifying and resolving a deficiency or failure.[11]

Another issue is the difficulty in finding processes by which the Federal government can effectively partner with the private sector in a collective sense, where each is a stakeholder, versus the normal model, in which the government is the buyer and industry is the supplier. Some believe Operation Warp Speed that delivered an effective COVID-19 vaccine in record time might be a good model to consider; regardless, this challenge requires creativity, a sense of urgency, and a willingness to challenge bureaucratic boundaries.

There is also a mismatch between the budgeting process and political will, and what is needed to devise and implement a viably strategy. Various reports have warned of uncertainty about funding, as a timely annual budget seems to have become a thing of the past; about policy, as new organizations are being created and existing ones changed; and about politics, which have become increasingly polarized, altogether make long-term planning and decision making challenging.[12] Strategy and planning should be conducted with a focus on risk and resiliency, but other considerations, such as cost and political expediency, may get in the way.

Finally, cultivating an adequate workforce, as in many areas of the United States economy, is a key concern.[13] For example, efforts to re-shore components of the ICT supply chain such as microchip production, face the obstacle of an insufficiently skilled, trained and scalable workforce.

D. Challenges Associated with New Technologies

The technology-driven diffusion and globalization of ICT supply chains is having a direct effect on the national security industrial base. For example, dependencies on offshore microchip production pose significant risks as evidenced by chip shortages during the

11. Ibid, at ii.
12. See, e.g., "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," Department of Defense, September 2018, p. 19. https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.
13. See, e.g., "Securing Defense-Critical Supply Chains: An action plan developed in response to President Biden's Executive Order 14017," Department of Defense, February 2022, pp. 47-53. https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.

II. Defense ICT Supply Chain Failures and Lessons Learned

pandemic. Our growing reliance on foreign sources of defense critical ICT makes it difficult to track the needs and vulnerabilities of the national security industrial base—and even to create a process and framework for doing so.

Additionally, the Biden administration and government experts are concerned that new technologies will be developed or "owned" by other nation-states, including adversaries, and that these countries will have an advantage in defining the rules for their use (such as standards-setting) or constrain U.S. access to these technologies.

However, new technological developments may make some elements of supply chain security management easier. For example, with some 200,000 companies providing elements for Pentagon weapons systems, it is difficult to ensure that each company meets all necessary security standards.[14] New technologies, such as artificial intelligence, machine learning and increased computing power may help aggregate, analyze and update key information about the supply chain, making it easier to understand and monitor it.

14. See, e.g., "Defense Industrial Base: DOD Should Take Actions to Strengthen Its Risk Mitigation Approach," Government Accountability Office, July 7, 2022. https://www.gao.gov/products/gao-22-104154; "Defense Procurement: Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership," Government Accountability Office, November 2019. https://www.gao.gov/assets/gao-20-106.pdf.

III. A Strategy for the Future

A. Assumptions About the Future

To be successful, a future strategy must effectively deal with known ICT risks, while also accounting for the evolving strategic environment and identifying the key characteristics expected to have a critical impact on the defense ICT supply chain. These characteristics comprise both technical and non-technical variables. Important trends include:

1. The nature of the geopolitical environment

At present, the United States finds itself in an era of strategic competition, where geopolitical tensions are likely to be more salient and there are greater risks of crises or even conflict—both between strategic competitors and in regional contexts. Strategic competition is likely to continue into the future, grow more complex and introduce greater geopolitical instability. In this emerging environment, specific crises in key regions (such as East Asia) will likely increase the risk of regional supply-chain disruptions and strategic competitors will seek opportunities to control and manipulate supply chains to our disadvantage.

2. Level and nature of economic interdependence

A common assumption is that levels of economic interdependence, even between rival states, will be maintained at high levels, if not grow. However, current trends call this assumption into question, especially with respect to ICT. Balkanization and polarization of political and economic relations are on the rise, with distinct blocs emerging and vying for regional and, potentially, global influence. The premises underlying the multilateral trading system created in the post-WWII era—that globalization of goods and services was not only highly desirable but also inevitable—are less certain and could transition to more regionally-focused trade arrangements with attendant restructuring of supply-chains.

3. National security as an imperative

A prevailing assumption over the past several decades is that the free market can, almost without exception, drive where—and at what price—we received the best value for goods and services. This assumption still holds true for huge swaths of the U.S. economy. However, regarding the acquisition or production of certain goods and services necessary for national security, over-adherence to this approach has at times resulted in problematic

III. A Strategy for the Future

outcomes for the defense industrial base, such as the unacceptable vulnerabilities the United States now confronts in the microelectronics industry.

4. **Technological change and dependence**

   Change is a given in the technological field, especially with respect to defense-critical ICT. It is also a given that the defense sector's use of and reliance on ICT will only grow. Consider, for example, the Secretary of the Army's strategic objective of making the Army "more data-centric and [able to] conduct operations in contested environments."[15] The military's consistent incorporation of, and growing reliance on technology generally, and ICT specifically, will increase the risks and potential impacts of supply-chain compromises and disruptions.

5. **Geopolitical Polarization**

   Current defense-critical ICT supply chains are built on a complex set of entrenched economic, political, financial, market and regulatory structures—among others. Necessary changes will depend on mustering sufficient political will within relevant domestic and international bodies and institutions to achieve consensus. Polarization and political gridlock, which are prevalent today, will likely continue to hinder both domestic and international efforts to implement changes and supply-chain restructuring. Therefore, future strategy should consider feasibility in implementation given the political conditions.

B. Desired End State: Uncompromised Access to Secure and Dependable Military Supplies and Capabilities

The Department of Defense's mission to provide combat-ready military forces, to deter war and protect the security of our nation, and to prevail in conflict if deterrence fails, cannot be compromised.[16] To meet this no-fail mission, the DoD must possess the technological and material advantages needed to succeed in crisis and conflict. The full array of capabilities, including defense platforms and weapons systems, needed to defend the nation must be available, secure and dependable at all times. The development and sustainment of these national security-critical capabilities requires secure, diverse, adaptable and resilient supply chains. Therefore, we require a future strategy that drives our desired end state.

15. Sec. Christine E. Wormuth, "Message from the Secretary of the Army to the Force," Army.mil, Feb. 8, 2022. https://www.army.mil/article/253814/message_from_the_secretary_of_the_army_to_the_force.
16. "About," U.S. Department of Defense, last retrieved March 5, 2023. https://www.defense.gov/about.

III. A Strategy for the Future

First, the defense ICT supply chain must rest upon a resilient and flexible supply chain that enables the DoD to reliably field, employ and sustain capabilities at whatever time they are needed. Second, it must be managed by a streamlined, multi-disciplinary decision-making process that not only includes internal DoD leaders and processes, but also easily integrates with other Federal Branch departments, civil research entities, and private sector ICT companies and financial entities. Third, the strategy must embrace and be comfortable with a planning and execution framework where the DoD can drive, influence and collaborate with the complex set of non-DOD ICT sectors that drive DoD risk.

Resilience is a dynamic objective; it reflects a state that must be continuously assessed and maintained within effective boundaries. In the context of this paper, resilience implies three things. The first is the resilience of the ICT supply chain itself: its ability to withstand and function despite disruptions through developing capabilities and processes to rapidly restore functioning and, when the former is not possible, ensuring reliable secondary and tertiary capabilities. The second is the operational resilience of the DoD to operate in the face of inevitable disruptions. The scope, scale and vulnerability of the DoD's supply chain means it is nearly impossible to secure each node. This makes operations resilience an essential element of the desired strategic end state. Finally, the strategy must drive strategic resilience across all aspects of national power (diplomatic, informational, military and economic) rather than solely relying on military options.

No matter one's perspective, reorienting our overall approach to defense ICT supply chains will be a long and difficult process. But to some extent, the imperative of focusing on resilience is already percolating into the strategy-making process. For example, in 2018, the United States issued its first National Space Strategy, which recognized that its adversaries had turned space into a warfighting domain.[17] As a result, survivability is now baked-in as part of the space acquisition process, with a new requirement of resiliency being an integral part of space procurement contracts.[18] The resourcing of the resiliency requirements has also been elevated as part of the Pentagon budget deliberations.[19]

17. President Donald J. Trump is Unveiling an America First National Space Strategy," The White House, March 23, 2018. https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy.
18. "Space Acquisitions: DOD Faces Significant Challenges as it Seeks to Accelerate Space Programs and Address Threats," Government Accountability Office, March 27, 2019. https://www.gao.gov/products/gao-19-458t.
19. Defense Budget Overview: United States Department of Defense Fiscal Year 2023 Budget Request, Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, April 2022. https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf.

IV. Guiding Principles for a Strategy

We have identified the following guiding principles that should direct a defense ICT supply chain strategy.

A. National Security Imperatives Will Sometimes Conflict with Free Market Principles.

As mentioned earlier, the United States government in general and the DoD in particular have an overriding requirement to protect the citizens of our country and to ensure our long-term security and prosperity. To meet its no-fail missions into the future, the DoD must have ready and reliable access to certain critical capabilities as well as the necessary strategies to mitigate risk and develop and sustain these capabilities. On balance, a strategy for the defense ICT supply chain should identify these capabilities and the specific products and services that support them, where uncompromised security and availability should be prioritized. This may be the inverse of what the balance should be for other aspects of the ICT supply chain—including other aspects of the defense supply chain that are not mission critical. However, a key challenge is that many, if not most, elements of the military supply chain touch the broader economy.

Achieving this will require the DoD to execute two related, but different approaches.

First, it will require a highly disciplined approach and a detailed understanding of systems, products and processes to identify what constitutes mission-critical ICT. This approach will enable strategists to identify the “no-fail” core assets and processes that hinge on the supply chain, versus those areas in which the DoD can accept more risk for a short or longer period of time. When defense ICT capabilities are vital to ensuring national security, free market principles should be appropriately balanced with ICT supply chain strategies, acquisition, or the development of critical defense ICT capabilities.

Second, the DoD must acquire the skills and personnel that are highly expert in all non-DoD ICT areas that the DoD is critically dependent upon. Again, the microelectronics supply chain offers a good example: the DoD needs to understand the implications of the CHIPS and Science Act, what it will fund, and how to ensure that the DoD gets access to the supplies they need. Simply, in order to oversee the process, as an interested customer, the DoD must have knowledge and insight into how all these elements are working together.

When there is a legitimate security reason to intervene in the free market, it should not be assumed that more money is always the solution. Sometimes it may require modifying regulations, creating incentives, or revising existing processes. In some cases, authorities

IV. Guiding Principles for a Strategy

may already exist. Consider, for example, the Defense Production Act (DPA) that can be leveraged when appropriate to secure essential products and services for our national defense, and that are not addressed by the market. In other cases, the U.S. Government may be an investor and actually own a stake or have some degree of control in a private-sector entity with national security impact.

B. Resiliency Should Be the Priority

Securing the U.S. defense industrial bases can be described, in part, as recalibrating the relationship between "defense" and "resilience." Defense implies a security posture that aims to prevent malicious actors from compromising the supply chain in the first place, while resilience implies a posture that accepts some inevitable level of compromise and instead directs resources toward redundant capabilities. Additionally, resilience is not one-size-fits all: sometimes it's a back-up plan, sometimes it's stockpiling, sometimes it's building redundancy capabilities. Regardless, a plan for resiliency should be added into acquisition requirements from the beginning.

Seeing that risk can never be totally eliminated, the focus should be on "buying down" as much risk as possible for those segments of the supply chain that have been identified as "no fail," and being willing to accept greater risk in areas of lower priority. For example, in some situations, it may be acceptable to rely on trusted partners or allies, rather than solely on internal capabilities. Indeed, it may be necessary because relying solely on domestic or home-grown solutions is a clear chokepoint—clearly identified even in non-defense related crises, such as last year's shortage of infant formula which is mostly domestically produced.[20] Identifying and then diversifying supply chains susceptible to these disruptions is the generally recommended policy: so-called "re-shoring" or "ally-shoring."[21] Nonetheless, this is often difficult to do in a cost-effective or timely manner. Consider, for example, recent efforts to decrease reliance on Taiwan and bolster U.S. chip manufacturing by building factories on American soil: it is an important effort, but it will take years for U.S. plants to become operational.[22]

20. "FACT SHEET: President Biden Announces Additional Steps to Address Infant Formula Shortage," The White House, May 12, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/12/fact-sheet-president-biden-announces-additional-steps-to-address-infant-formula-shortage.
21. Elaine Dezenski and John C. Austin, "Rebuilding America's Economy and Foreign Policy with 'Ally-Shoring,'" Brookings, June 8, 2021. https://www.brookings.edu/blog/the-avenue/2021/06/08/rebuilding-americas-economy-and-foreign-policy-with-ally-shoring.
22. See, e.g. Catherine Thorbecke, "Micron to Invest Up to $100 billion to Build Chip Factory in Upstate New York," CNN, Oct. 4, 2022. https://www.cnn.com/2022/10/04/tech/micron-100-billion-chip-factory-new-york/index.html.

IV. Guiding Principles for a Strategy

C. Identifying Things Beyond DoD Control and Planning for Them

The DoD can, in theory, secure the aspects of its supply chains over which it has direct control. But the reality is that it cannot secure everything at all times, and the DoD is increasingly dependent on the broader global market. Moreover, the DoD is a relatively small player in the global marketplace, which limits its leverage and standard-setting power. However, the DoD can identify opportunities and policy options that increase U.S. government leverage in a global marketplace. Therefore, there may be a tension between what the DoD defines as "mission critical" and of the highest priority, and whether the DoD even controls those parts of its supply chain. This creates an imperative to identify those things that are beyond the control of the DoD but that remain central to its effectiveness, and to calculate and mitigate those external risks.

D. Creating an Enduring "Demand Signal" for Security

The most secure option is often not the fastest or cheapest one. Instead, security often requires long-term, disciplined planning and investment. Given the style of U.S. democracy and its frequent pivots between policies and parties, there is a risk that policy will change over time as administrations change, creating an uncertain environment for the defense industrial base and also undermining long-term efforts.

As such, it is likely that an enduring "demand signal" for security will only be effectively created by enshrining it in law, thus creating a role for Congress to weigh in within a context of multiple stakeholders, including business and industry, the public, and the defense sector. Doing so will also help create a policy with "teeth"— that is, one that includes mechanisms for accountability. This requires enduring political interest and attention, particularly on the part of lawmakers. Without the political will to create and enforce meaningful standards to improve supply chain security, the strategy will not have an enduring impact.

IV. Guiding Principles for a Strategy

E. Ensuring Flexibility

This call for a strategy is future-oriented: it focuses on issues of the present—the strategic issues we currently understand—and of the future—those problems which we anticipate. It does so because we recognize that the problems of today are often a product of outmoded thinking or past failures of incentive, imagination, or resourcing. However, each and every strategy—even future-focused ones—will, at some point, itself become outdated.

A strategy, therefore, should offer a framework to expect the unexpected. Specifically, a strategy to secure the defense ICT supply chain should articulate a recurring process to assess progress, objectives, and priorities and enable adjustments as needed, to include off-cycle changes that may need to be implemented as a result of new circumstances.

F. Getting Ahead of the Pace of Technological Change

There are two issues stemming from the pace of technological change. The first is whether the United States has a forward-leaning posture to anticipate emerging technological capabilities, and to decisively engage with the processes to acquire them. The second is anticipating the vulnerabilities that may arise from these new technologies (or from the interaction of legacy and new capabilities) that could be exploited for malicious purposes.

A more forward-thinking defense strategy expects that security needs now will evolve alongside new technological developments and will plan accordingly. Such a strategy should also offer a continuous method to evaluate the significance of emerging threats in order to determine the nature and severity of an enduring threat to make sure we do not lose sight of broader objectives.

The United States will also need to take a global leadership role in setting the rules for how and when these technologies will transform the supply chain. Part of this will require balance and engagement on the international level to ensure the technical standards or specifications for key technologies are ones that promote security. The alternative is similar to the stress, confusion and lack of competitive advantage associated with the standards-setting process for 5G.[23]

23. For concerns about falling behind, see e.g. Arjun Kharpal, "China 'Has the Edge' in the War for 5G and the US and Europe Could Fall Behind," CNBC, March 7, 2018. https://www.cnbc.com/2018/03/07/china-has-the-edge-in-the-war-for-5g-us-and-eu-could-fall-behind.html; for competition over standards, see e.g. Alexandra Bruer and Doug Brake, "Mapping the International 5G Standards Landscape and How It Impacts U.S. Strategy and Policy," Information Technology and Innovation Foundation, Nov. 8, 2021. https://itif.org/publications/2021/11/08/mapping-international-5g-standards-landscape-and-how-it-impacts-us-strategy.

IV. Guiding Principles for a Strategy

We must also account for the potentially limited role of the military in setting norms in this space and identifying which stakeholders in the federal government and industry are essential for promoting effective norms. Promoting and protecting U.S. innovation and intellectual property will be a key component of this challenge.

G. Adapting Procurement and Budgetary Policy for a New Era

Many current acquisition laws and policies are a legacy of a different age, maladapted to the current and future security and technology environments. For example, budgetary and procurement structures often lack the speed and agility to adequately predict and mitigate supply-chain risks, which may slow down defense actions or foster rigidity. Authorities may not take into consideration the increased speed of modern information flows or the need for quick decision-making.

There are, however, examples of older processes being adapted to meet the present need. For example, the Defense Production Act (DPA) was enacted in 1950 right after the start of the Korean War.[24] The current version of the law still gives the Executive Branch substantial powers, empowering the President to "allocate materials, services, and facilities" for national defense purposes.[25] Most recently, Presidents Donald Trump and Joseph Biden have both invoked the DPA in response to the COVID-19 pandemic and associated supply chain challenges—though not without controversy.[26]

As a future guiding principle, Congress will need to reexamine current authorities and processes and potentially authorize new procurement and budget policies to enable speed and agility in helping mitigate future supply chain risks. By way of example, Other Transactional Authority (OTAs) have proven to be a viable means to speed the demand signal to industry and hasten production of necessary goods and services to the government and may also be leveraged, as appropriate, while a review of existing laws and policies is assessed to support production agility.[27]

24. "Defense Production Act," Britannica, last updated May 2022. https://www.britannica.com/topic/Defense-Production-Act.
25. "Defense Production Act Authorities" Federal Emergency Management Agency, last accessed Dec. 1, 2022. https://www.fema.gov/disaster/defense-production-act/dpa-authorities.
26. Gavin Bade, "Trump Expands DPA, Amid Mounting Pressure," Politico, Apr. 2, 2020. https://www.politico.com/news/2020/04/02/trump-expands-dpa-order-162128; Myah Ward, "Biden Invokes Defense Production Act to Increase Supply of U.S. Infant Formula," Politico, May 18, 2022. https://www.politico.com/news/2022/05/18/biden-invokes-defense-production-act-to-increase-supply-of-u-s-infant-formula-00033618.
27. Rhys McCormick, "Department of Defense Other Transaction Authority Trends: A New R&D Funding Paradigm?" Center for Strategic and International Studies, Dec. 8, 2020. https://www.csis.org/analysis/department-defense-other-transaction-authority-trends-new-rd-funding-paradigm.

IV. Guiding Principles for a Strategy

H. The Imperative of Constant Vigilance

Ensuring the availability, security and resilience of defense-critical ICT is an ongoing concern that demands vigilance. It requires an operational approach and mindset to consistently monitor the supply-chain and adapt priorities, processes and actions to address new vulnerabilities, threats and shortfalls. A future strategy should account for this imperative, drive continuous attention and provide mechanisms to hold leaders accountable throughout the chain of responsibility. A key component to this is making sure that robust oversight mechanisms, both internal and external to the DoD, are utilized as necessary to ensure compliance with governing law and policy. Effective implementation and execution of the strategy and operations are also necessary.

V. Implementation and Next Steps

Most defense ICT supply chain analyses focus on immediate to mid-term challenges and offer recommendations that apply along similar timeframes.[28] In calling for a future-focused strategy, the goal is to orient thinkers toward a broader, longer-term strategy that is proactive rather than reactive, and that can endure across the years while remaining flexible.

That said, there are aspects of such a strategy that, despite being future-focused, could be implemented in the shorter term. For example, revising procurement and acquisition policy that considers security at the outset and incorporates resilience concepts could be initiated now. Conversely, cultivating the political will necessary to create a demand signal for security may take longer.

Ultimately, this is a job that requires multiple stakeholders to work together. The phrase "whole-of-government" may be overused, but describes the pattern of legal changes, government incentives, industry buy-in and executive action that are needed to realize the goals detailed in this report.

The U.S. defense industrial base supply chain is unacceptably vulnerable. Recent wake up calls that have revealed the fragility of supply chains, such as the COVID-19 pandemic, have been important in shedding light on current challenges. However, policymakers continue to focus on remediating existing issues rather than tackling the more vexing challenge of anticipating and addressing new ones. The reality of the volatility of the current geopolitical environment and the dynamic nature of technological change only underscore the salience of improving the defense and resilience of the ICT supply chain. While ongoing efforts to address existing vulnerabilities are important, this should not come at the expense of shifting to a longer-term perspective to identify and future challenges.

28. See, e.g. "Securing Defense-Critical Supply Chains: An action plan developed in response to President Biden's Executive Order 14017," Department of Defense, February 2022, pp. 54-57. https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF; and "Supply Chain Security Strategy, Appendix 1 to DLA's 2018-2026 Strategic Plan," The Defense Logistics Agency, 2018, p. 2. https://www.dla.mil/Portals/104/Documents/Headquarters/StrategicPlan/SupplyChainSecurityStrategy.pdf.

Author Biographies

Gary Corn	Director of the Technology, Law & Security Program at American University's Washington College of Law, and former general counsel for U.S. Cyber Command
Erica Lonergan	Assistant professor in the Army Cyber Institute at the United States Military Academy at West Point
Mary Brooks	Former fellow for R Street's Cybersecurity and Emerging Threats team

WORKING GROUP MEMBERS:

Rick Ledgett	Former deputy director of the National Security Agency.
Bradley Martin	Director of the RAND National Security Supply Chain Institute
Kevin McLaughlin	Former deputy commander of U.S. Cyber Command
Kevin Meiners	Former deputy undersecretary of defense for intelligence in the Department of Defense
Robert Taylor	Former principal deputy general counsel for the Department of Defense

Appendix A

List of key reports from the past five years on the military ICT, national security and/or defense industrial base supply chain:

- "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States" Department of Defense, September 2018, pp. 45-51. https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.
- "Building a Trusted ICT Supply Chain," Cyberspace Solarium Commission, October 2020. https://www.solarium.gov/public-communications/supply-chain-white-paper.
- Caolionn O'Connell, et al. "Managing Risk in Globalized Supply Chains," RAND Corporation, 2021. https://www.rand.org/pubs/research_reports/RRA425-1.html.
- Chris Nissen et al., "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," MITRE, Aug. 3, 2018, p. ii. https://www.mitre.org/news-insights/publication/deliver-uncompromised-strategy-supply-chain-security-and-resilience.
- "The Final Report," The National Security Commission on Artificial Intelligence, March 2021. https://www.nscai.gov/2021-final-report.
- "Fiscal Year 2020: Industrial Capabilities Report to Congress," Department of Defense, January 2021. https://media.defense.gov/2021/Jan/14/2002565311/-1/-1/0/FY20-INDUSTRIAL-CAPABILITIES-REPORT.PDF.
- "H.R.4346 - 117th Congress (2021-2022): Chips and Science Act," Library of Congress, Aug. 9, 2022. https://www.congress.gov/bill/117th-congress/house-bill/4346.
- "Report of the Defense Critical Supply Chain Task Force," House Armed Services Committee, July 22, 2021, p. 13. https://web.archive.org/web/20220712210401/https://armedservices.house.gov/_cache/files/e/5/e5b9a98f-9923-47f6-a5b5-ccf77ebbb441/7E26814EA08F7F701B16D4C5FA37F043.defense-critical-supply-chain-task-force-report.pdf.
- "Securing Defense-Critical Supply Chains," Department of Defense, February 2022, pp. 54-57. https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.
- "Supply Chain Security Strategy, Appendix 1 to DLA's 2018-2026 Strategic Plan," The Defense Logistics Agency, 2018, p. 2. https://www.dla.mil/Portals/104/Documents/Headquarters/StrategicPlan/SupplyChainSecurityStrategy.pdf.