WAR BY OTHER LEDGERS

A COMPILATION OF ARTICLES ON MODERN ECONOMIC STATECRAFT

Editors

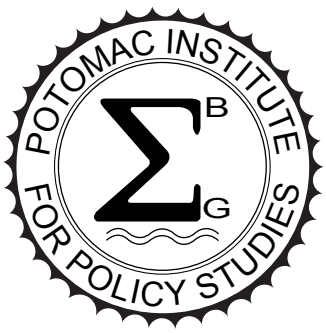
Tim Welter, Jennifer Buss, Kimberly Sloan

POTOMAC INSTITUTE FOR POLICY STUDIES

WAR ON THE ROCKS

WAR BY OTHER LEDGERS

NONPARTISAN
S&T POLICY



Convener. Connector.
Trusted Partner.

THE POTOMAC INSTITUTE FOR POLICY STUDIES

Providing foundational foresight that transforms complexity into clarity, and clarity into action.

ABOUT THE POTOMAC INSTITUTE FOR POLICY STUDIES

The Potomac Institute for Policy Studies is an independent, nonpartisan, 501(c)(3), non-profit science and technology policy research institute. The Institute identifies and leads discussion on key science and technology issues facing our society. From these discussions and forums, we develop meaningful policy recommendations and ensure their implementation at the intersection of business and government.

ABOUT THE GLOBAL COMPETITION PROJECT

The Potomac Institute for Policy Studies regularly engages with a spectrum of experts to elevate insights on the primary challenges and opportunities associated with technology policy and national security. The Institute's Global Competition Project (GCP), founded in 2021, focused on societal level competition, develops foundational references for national security professionals, policymakers, industry leaders, and others while driving awareness in how the U.S. might address the most consequential aspects of the globally competitive environment. The Project has delivered on that goal through its research, publications, panels, and continuous dialogue, all through the lens of the Institute's mission intersecting science and technology, business, and government.

Some content in this volume reproduced with permission by *War on the Rocks*.
Article references active as of *War on the Rocks* publication date.

Thank you to Potomac Institute for Policy Studies' Senior Fellows, Researchers, and Staff and to *War on the Rocks* authors and editors for their contributions to this work. Special thanks to Potomac Institute for Policy Studies' interns Bradley Olson (George Mason University), Vanessa Neubauer (George Mason University), and Samuel Harlow (George Washington University) for providing research contributions and administrative support.

FURTHER INFORMATION AND PERMISSIONS MAY BE REQUESTED FROM:

Potomac Institute for Policy Studies
Email: info@potomacinstitute.org

© 2026 Potomac Institute for Policy Studies. All Rights Reserved.

This work may be shared and distributed with proper attribution to the Potomac Institute for Policy Studies. No copying, translation, or adaptation is allowed without written permission from the Potomac Institute for Policy Studies.

DISCLAIMER: The Potomac Institute for Policy Studies cannot be held responsible for errors or any consequences arising from the use of information contained in this publication. The views expressed here are those of the author(s) and do not necessarily reflect those of the Potomac Institute for Policy Studies. The Potomac Institute is nonpartisan and does not advocate for partisan, political agendas.

Potomac Institute for Policy Studies
901 N. Stuart Street, Suite 1200
Arlington, Virginia 22203
Phone: (703) 525-0770
Fax: (703) 525-0299
www.potomacinstitute.org

TABLE OF CONTENTS

PREFACE		2
INTRODUCTION	Economic Statecraft is Back. Is America Ready?	4
CHAPTER 1	Sun Tzu in the Supply Chain: The New Face of Economic War with China	8
CHAPTER 2	Economic Statecraft and the Federal Institutional Architecture	18
CHAPTER 3	Fighting an Economic War Without Fused Intelligence	26
CHAPTER 4	Follow the Money: Finance and the Future of Allied Economic Statecraft	36
CHAPTER 5	Sharpening Signals and Reducing Noise for Better Defense Budgets	46
CHAPTER 6	Operationalizing Economic Statecraft: A New Imperative for the Pentagon	56
CHAPTER 7	Seeing the Cyber in Economic Statecraft	60
CHAPTER 8	Rethinking Corporate Risk and Alignment in an Era of Economic Statecraft	70
CHAPTER 9	Rebuilding American Manufacturing: A Keystone for Economic Statecraft	78
CHAPTER 10	Academia's Critical Role in Developing an Economic Security Workforce	86
CHAPTER 11	Writing the Playbook: A Strategy and Doctrine for American Economic Security	96
ENDNOTES		102

PREFACE

This *War by Other Ledgers* book grew out of several years of work initiated under the Potomac Institute for Policy Studies' Global Competition Project (GCP). The GCP seeks to identify, elevate, and address strategic issues vital to the United States' competitive posture through research and engagement across government, the private sector, and with allies and partners.

Now more than ever, economic security is inseparable from national security, and economic statecraft is the means by which nations pursue strategic interests on both fronts. An 11-part article series with *War on the Rocks* was inspired by the need to provide a better understanding of the various facets of contemporary economic statecraft so public and private sector leaders can better navigate the geostrategic environment, address risks, and leverage opportunities through policy and practice that support enduring U.S. economic security.

By no means a new instrument of national power, economic statecraft today must reconcile with a global environment that is hyperconnected virtually and physically. The technology-enabled flow and ubiquitous access to information has created era-unique interdependencies, including global supply chains and markets, unprecedented in human history — a source of risks and opportunities.

Progress is underway across the public and private sectors to mitigate those risks and capitalize on the opportunities. New policies, practical concepts, and institutional initiatives have emerged as recognition grows that economic statecraft is a vital strategic and operational discipline. But much of that work remains

disparate, disconnected from each other and from a guiding vision orchestrated toward defined strategic ends. No common definition of economic statecraft guides the federal government, authorities are scattered across departments, and the workforce trained to use them is still emerging. The private sector is equally grappling with how best to navigate the new terrain.

When *War on the Rocks* invited the Institute to produce a series of papers on contemporary economic statecraft, these developments and opportunities became the series' backbone. The project brought together practitioners and scholars from government, the military, industry, academia, and partner nations to help clarify the field and contribute practical ideas for its continued development.

This book's chapters expanded on the 11-part collaborative article series, exploring how the United States might evolve various aspects of contemporary economic statecraft into strategy and practice. It is neither exhaustive nor complete, but rather a work in progress and an initial attempt at understanding the state of play and where we need to go. Each chapter includes a brief abstract, while selected chapters include an epilogue and QR code linking to a corresponding webinar online.

Taken together, the chapters describe a discipline still taking shape. Our hope is that they also mark a starting point for the doctrine, organization, and professional pipeline economic statecraft requires to deliver security and prosperity for the nation.

INTRODUCTION



Scan the QR code to view the articles on the Potomac Institute for Policy Studies website.

ECONOMIC STATECRAFT IS BACK. IS AMERICA READY?

Nicholas Hanson and Madeline Field

In 432 B.C.E., a year before the outbreak of the Peloponnesian War, the Megarians received an unusual decree from the Athenian assembly: They were prevented from accessing the vast Athenian Empire's harbors and marketplaces due to their alliance with Sparta, a rising empire that posed a clear threat to Athens' hegemony.[1] While the official reasoning is lost to history, many scholars believe that Athens, fearful of the rising great power, used sanctions to force Megara's economic decline.

So began the deliberate use of economics as a tool of statecraft.

In the millennia since, economics remained an important enabler of state power.[2] Yet over the course of the 20th century, the tools of economic statecraft transformed in response to globalization and its gnarled, twisted webs of overlapping capital markets, supply chains, multinational commercial banks, and international organizations.[3] Economic statecraft has quickly become more critical than ever.

Since World War II, the United States has shaped both global governance and the international economic order, as it boasts the world's most powerful economy.[4] The U.S. dollar serves as the world's reserve currency.[5] Together, America's strong economy and the dollar's exorbitant privilege have allowed it to unilaterally wield economic weapons against its foes while rarely being the target.[6] Yet that postwar dynamic has shifted significantly in the past decade. This is in part due to "America First" politics, which broadly seeks to renegotiate the terms of U.S. economic engagement with the rest of the world, but also from China's rise as America's primary strategic competitor.[7] A manufacturing superpower and the world's second-largest economy, China's behavior contradicts its common refrain that it is participating in a win-win "community of common destiny."[8] Rather, experts believe that China — and arguably the United States — is playing a zero-sum game at the rest of the world's expense.[9]

China and America each draw their international political power from the strength of their economies and access to capital markets, and throughout the aughts, there was a sense that the two countries could together build a more prosperous world.[10] Yet in the past decade, both countries have begun to exert their economic leverage, and the economic relationship between the United States, China, and the rest of the world has instead become outright coercive.[11] And industry, both directly affected by economic statecraft and critical to its success, is on the frontlines.[12]

In the past several years, China has expanded its economic statecraft toolset: restricting access to critical minerals supply chains, opening up antitrust investigations of U.S. tech companies, ramping up its well-known intellectual property theft (increasingly enabled by cyberattacks), and increasing strategically significant investments in wealthy countries.[13] The United States, too, has expanded its economic statecraft policy options. In addition to maintaining its crippling sanctions regime, it has

sought access to critical minerals, tightened some restrictions on foreign investments, introduced new limits on the imports of strategic resources in the defense supply chain, aggressively pursued reindustrialization, and slapped large tariffs on friend and foe alike.[14]

While current economic statecraft policy is at times bewildering, there is no doubt that the cost of losing ultimate economic leverage is high. In America, increased economic pressure from China would lead to higher prices, goods shortages, and ultimately, slow growth.[15] More broadly, it will lead to a more neo-mercantilist and illiberal future. America, and its friends — if they are still friends — will ultimately suffer.[16]

Yet despite an increased reliance on economic tools to accomplish national security objectives and the high stakes, America is unequipped to address China and other threats to its economic security.

Currently, there doesn't seem to be a whole-of-government economic statecraft policy driving decisions. While economic statecraft assumes a central role in the Trump administration's 2025 National Security Strategy, the document is short on specifics.[17] Similarly, the Fiscal Year 2026 National Defense Authorization Act contain few allusions to it, with a few exceptions.[18]

The Defense Department has emerged as a potential coordinating agency in focusing heavily on important economic security issues: supply chain vulnerabilities, the availability of critical materials, cybersecurity, and emerging technologies.[19] Efforts to further empower the Office of Strategic Capital and stand up the new Economic Defense Unit indicate that the department is serious about these threats.[20]

Yet the Defense Department has generally been separated from the traditional instruments of economic statecraft wielded by the Treasury, Commerce, and State Departments. Without a more defined role handed to the Defense Department by Congress or the White House, its impact is limited. Such ambiguity within the U.S. government does not send strong demand signals to industry partners, enable strategists to begin developing tools and networks for successful policy, or lay the bedrock for effective inter-agency coordination.

Americans haven't had to consider a post-liberal world in decades, much less what weaponized interdependence would do to the international economic order.[21] It is perhaps unsurprising, then, that consequential, uncomfortable questions have largely gone undiscussed: *What does an economic security doctrine look like for the Defense Department? What agencies or departments own the problem set, and how can they receive funding? How may governments and private industry interact or share business intelligence? How can industry be incentivized to cooperate with the Defense Department? If economic statecraft fits in the Defense Department, what consideration for economic statecraft should be given across the planning, programming, budgeting, and execution process, and who is responsible for coordination and alignment?*

America needs a broader strategy, and that starts with an informed conversation. Concerned about the existential stakes of this issue, the Potomac Institute for Policy Studies and *War on the Rocks* are teaming up to elevate this debate. This special series will seek to answer those questions and more in a series of 11 articles, each building upon the last. While these authors will provide some high-level policy recommendations, they are in no way intended to be exhaustive solutions to complex, billion-dollar problems.

We're extremely excited to partner with the Potomac Institute on this important effort.[22] The Potomac Institute — a leading science and technology policy research center at the intersection of government and business — has been behind the scenes coordinating these discussions for several years. They've brought to bear their network of experts, and other representatives of this small but passionate community, and we encourage you to explore their research on these topics.[23]

This is a perilous time for the United States and its allies, as we all navigate a more uncertain world.[24] The team at *War on the Rocks* hopes you'll feel as concerned and inspired by these challenges as we do.

Nicholas Hanson is the chief operating officer of *War on the Rocks*.

Madeline Field is the assistant editor of *Cogs of War*, a vertical at *War on the Rocks* focused on defense technology and the defense industrial base.

Americans haven't had to consider a post-liberal world in decades, much less what weaponized interdependence would do to the international economic order.

CHAPTER 1

ABSTRACT

A competition between China and America has played out predominantly in the economic domain, often characterized by China's adversarial practices and lack of a coherent American counterstrategy. The Chinese Communist Party's deliberate strategy to steal and use intellectual property and technologies to develop and accelerate their industrial base, and subsequently overtake U.S. markets, have resulted in economic leaps that translate into military advantages that undermine American national security. While evolving, existing U.S. policy, law, and institutions across the public and private sectors lack the structural support necessary to carry out effective economic statecraft holistically.

The authors posit that the United States must develop a coherent, societal-level approach to economic statecraft to ensure its enduring prosperity and security. Such an approach must include mobilizing the government, increased military vigilance, and incentivizing the private sector to act in concert with U.S. strategic objectives to realize the effective exercise of economic statecraft.

Scan the QR code to view the webinar that accompanies Chapter 1.

Pierre Marshall/CC BY 4.0

SUN TZU IN THE SUPPLY CHAIN: THE NEW FACE OF ECONOMIC WAR WITH CHINA

Tim Welter and Margaret McWeeney

The United States loses upwards of $225-$600 billion each year to stolen trade secrets, pirated software, and counterfeit goods, mostly through activities orchestrated by China's government.[25]

Right now, the two countries are locked in a struggle that looks nothing like the wars of the past. The stakes are existential with prosperity and national security on the line, not to mention global influence. This is an economic war, and it's being fought according to principles that date back more than two millennia.[26]

Economics is no longer just a lever of national power — it is an operational domain of warfare and economic statecraft provides an effective means to operate in that domain. Defined broadly, economic statecraft is the use of economic tools — trade policy, investment controls, and sanctions — to achieve strategic objectives.

The United States and China are engaged in a protracted economic conflict, and America's approach to dealing with it is evolving. The Chinese Communist Party's primary goal to stay in power drives its wielding of economic tools to sink U.S. industries and gain market advantages — a reality American policymakers are actively grappling with. Military commanders and national security professionals should understand the dynamics of economics if they expect to gain advantage, deter, and win, if necessary, on the modern battlefield.

The timeless maxim attributed to Sun Tzu — "The supreme art of war is to subdue the enemy without fighting" — has found new life in the 21st century.[27] In 1999, two People's Liberation Army officers published *Unrestricted Warfare*, a book that argued for a broader conception of war.[28] Their thesis: Modern conflict transcends the battlefield. Financial systems, trade networks, and information flows can be weaponized in a broader societal approach to war to achieve strategic aims without firing a shot.

While *Unrestricted Warfare* is not official Chinese doctrine, its influence is undeniable. It echoes through Beijing's policies and ambitions, both hidden and unhidden. China's Belt and Road Initiative, for example, binds dozens of countries into a web of infrastructure and trade relationships, while *Made in China 2025* outlines a path to dominate high-tech sectors, from AI to advanced manufacturing.[29] Ambitious military modernization has complemented these efforts, ensuring that economic power translates into geopolitical leverage.[30] These pursuits are not mere economic plans — they are instruments of China's national power, wielded to secure its rise and reshape global norms in its favor while keeping the communist regime in power.

It's All About the Party

For the Chinese Communist Party, economic dominance is not a byproduct of growth. It is a deliberate strategy pursued vigorously across a wide spectrum, from coercion and obfuscation to seemingly innocuous compliance with global norms, always with the survival of the Party's rule at the forefront. Since 2006, the Party's successive five-year plans have prioritized science and technology innovation,

self-reliance, and global competitiveness.[31] The goal is clear: reduce dependence on foreign powers, control critical supply chains, and position China as the world's preeminent economic and technological force.

Contrast this with the United States: For decades, Washington viewed economic engagement with China as a win-win proposition. American policymakers assumed that integrating China into the U.S. and other global markets would liberalize its politics and create mutual prosperity. By failing to understand Chinese culture and strategy and mirror-image its assumptions, America underestimated the Chinese Communist Party's resolve to maintain power and pursue its goals. As Zachary Karabell observed in *Superfusion*, the United States helped create the China it now faces.[32] While both countries certainly prospered and hundreds of millions of Chinese were raised out of abject poverty, Beijing's path exploited the openness of U.S. and global markets along the way.[33] The consequences of this misreading become clear when China's leverage of U.S. and allied systems is examined across certain sectors.

In the 1990s, Chinese researchers became deeply embedded in Western academic and research ecosystems, particularly in telecommunications, leveraging open scientific norms to absorb innovation and transfer it to state-linked firms.[34] Open access to academia enabled trade-secret theft, coerced technology transfer, and standards manipulation.[35] Backed by massive state support, political top cover, and protected domestic markets, Chinese firms could scale quickly, underprice competitors, and dominate global markets while excluding foreign rivals domestically. U.S. markets were aggressively undercut and collapsed in the melee, with domestic manufacturing in key strategic areas — solar panels, lithium-ion batteries, wind energy components, and electric vehicles — caught in the crossfire. As a result, in a relatively short time, China gained notable competitive advantages militarily, economically, and technologically on the global stage. The commercial drone industry illustrates how this strategy unfolds.

U.S. Drone Market Shot Down

China absorbs foreign technological advances, converts them into industrial capability, and leverages state support to dominate markets. Their pattern of behavior tends to exclude U.S. competitors and uses new market advantage to threaten U.S. security. The erosion of U.S. advantage in drones and its subsequent exclusion, provides an example.

In the early 2000s, the United States and its allies led drone innovation, driven by dual-use military research, academic robotics programs, and a hobbyist and startup ecosystem. Chinese firms exploited this open environment through academic exchange, appropriation of publicly funded research, and reverse engineering, enabling the transfer of critical knowledge from Western universities and firms into China's industrial base.[36]

At the industry and state level, China translated this appropriated knowledge into market capture, through firms such as DJI, which came to dominate more than 70 percent of the global commercial drone market by the late 2010s.[37] These advantages allowed Chinese firms to underprice and outscale U.S. competitors, consolidate control over drone manufacturing, software ecosystems, and data platforms, and ultimately lock American firms out of both the Chinese market and key global supply chains.

This model of intellectual property appropriation, rapid scaling, and market exclusion — done largely through nominally nonstate firms — generated two main durable strategic advantages for China at relatively low cost. First, it introduced significant vulnerabilities for the United States across critical mineral and component supply chains, including rare earth elements, lithium-based batteries, specialty magnets, sensors, and electronics essential to unmanned systems. Chinese dominance across multiple nodes of these supply chains enables leverage over pricing, availability, and downstream manufacturing, increasing U.S. exposure to disruption in both commercial and defense sectors. Second, because drones play a central role in intelligence, surveillance, reconnaissance, and precision-strike operations, China's

leadership in drone technologies and in the critical minerals and components confers potential battlefield advantages. China is reported to be expanding its drone deployment capacity, with low-cost systems increasingly proliferating across conflict zones.[38] In some cases, drones provided by the People's Liberation Army to local partnered forces have subsequently entered into the hands of hostile actors, including terrorist groups, elevating the risk of threats to U.S. personnel, infrastructure, and assets overseas.[39] The drone sector thus demonstrates how adversarial economic statecraft can undermine U.S. national security, transforming what begins as commercial competition into concrete threats to both economic resilience and military security.[40] This pattern ripples across many sectors critical to U.S. national security.

America Reconciles with China's Reality

The 2018 National Defense Strategy marked a significant pivot for the United States from the decades-long post-9/11 focus on counterterrorism, acknowledging "great power competition" as the new defining challenge of the era.[41] A competition, however, implies a level playing field and shared rules — not the rules China was playing by. A systemic shock would make the imbalance unmistakable.

Indeed, it took the global shortages of medical equipment and pharmaceutical ingredients during the COVID-19 pandemic to highlight the grave risks created by heavy U.S. reliance on Chinese manufacturing hubs and key supply chains.[42] The pattern of structural dependence, however, long predated the pandemic and is particularly evident in critical mineral supply chains — including rare earth elements, lithium, cobalt, and graphite — and is combined with state-backed overseas investment, multi-year contracts, and downstream-processing dominance. These dynamics are further reinforced through infrastructure finance (including inside the United States) and development projects such as the Belt and Road Initiative.[43] Regardless, the pandemic initiated a sudden and stark realization of the supply chain chokeholds China had on the United States and its willingness to leverage that advantage, serving as a catalyst for a broader strategic reckoning.

The Biden administration's 2022 National Defense Strategy generally echoed the competitive sentiment of its 2018 Trump predecessor, transcendent of political party lines.[44] The rhetorical repetition reflected wider realization and rare consensus among policymakers and others about the real threats China posed: not competition, rather, a war fought in boardrooms, with supply chains, and in research labs. A war where victory means shaping the future of technology, trade, and global governance. In other words, economics as a domain of warfare — sometimes also called gray zone aggression, hybrid warfare, or adversarial economic statecraft — is experiencing a contemporary resurgence with unique 21st century attributes. The question then becomes how the United States should organize to fight in that domain.

Carl von Clausewitz proposed that the aim of war is to disarm the enemy.[45] Today, disarmament occurs without kinetic force. Entire U.S. industries, including those with critical military relevance, have vanished under the weight of Chinese manufacturing dominance. Key technologies, strategic materials, and infrastructure have been captured, not by force of arms, but by force of economics. Jobs have disappeared. Supply chains have fractured. Vulnerabilities have multiplied. Across multiple industries and domains, China has demonstrated a recurring, evident pattern that threatens American prosperity, including attracting foreign capital and expertise, coercive or illicit acquisition of intellectual property, leverage over infrastructure, coercive regulatory pressure, state–private–criminal blending, and disruption.[46] These developments underscore why economics should be treated as a core function of modern warfare.

This is classic Sun Tzu in action: Know your enemy, know yourself, and you need not fear the outcome of a hundred battles. Beijing studies America's strengths — and its weaknesses. What Americans view as strengths, such as relatively open U.S. markets and a fragmented political system of representative democracy, has been exploited with precision by China, along with vulnerabilities from reliance of the U.S. economy and military strength on global supply chains. As such, if you control your adversary's access to critical technologies, rare earth minerals, or global markets, you have

effectively neutralized their ability to act strategically — militarily or economically — presenting existential threats. This is the essence of contemporary economic warcraft: enduring, non-kinetic, and deeply integrated into daily geostrategic activity with consequences that can rival or exceed those of traditional warfare.

The Path Ahead: Economic Statecraft

The deliberate exercise of economic statecraft offers a way forward. This includes industrial policy, manifested recently by U.S. investment in publicly traded companies like Intel and critical minerals firms to protect resources and technologies important to national security.[47] Wielding these tools effectively requires more than tariffs and export bans. It demands sound strategy, coherent doctrine, clear authorities, and robust public-private partnerships.

Successive annual defense authorization bills have included meaningful legislation like the Creating Helpful Incentives to Produce Semiconductors Act of 2022, giving intent and direction on economic statecraft from Congress, supported by the House Select Committee on Competition with China, the U.S.-China Economic and Security Review Commission, and others in the policy ecosystem.[48] The Trump administration has issued parallel guidance in executive orders and in the recent 2025 National Security Strategy.[49] The strategy highlights the economy as the foundation of U.S. global posture supported by a strong, well-equipped, and ready military. And while the peace-through-strength-equals-deterrence approach is not new, how to operationalize it given the complexities of modern geopolitics, tightly woven global supply chains and markets, and unprecedented information hyperconnectivity, is yet to be coherently addressed. The limiting factor is not policy ambition, but institutional design. The next step, therefore, lies in fixing structural weaknesses within the U.S. system while holding true to national values.

The United States lacks a dedicated authoritative body at the strategic level to proactively identify and analyze economic threats to vital supply chains, and to prioritize and share those findings appropriately across industry, academia, the business sector, the federal government, and then partner with parties from across those areas to act on those threats with relevant authorities, speed, and effectiveness. A central challenge is not a lack of data, but a lack of analytic integration across space and time. This fragmentation obscures patterns, delays attribution, and leaves policymakers and agencies reacting to individual events instead of disrupting activity at its source.

The United States also lacks a systematic, integrated framework for understanding and addressing China's holistic military-civil fusion approach to statecraft.[50] While effective work is being done to counter economic-based threats, be it at Treasury, Commerce, or the Department of Defense, the approach is piecemeal. Without such a framework and an entity to referee, responses will remain reactive, episodic, and disparate across the U.S. government, and detached from a broader unifying strategy.

These gaps have direct implications for military readiness and deterrence.

The Military Challenge

Vigilance by U.S. military commanders should therefore span beyond air, sea, space, land, and cyber to identify indications and warnings of economic vulnerabilities to military operations and capabilities. At risk is unfettered access to supply chains that enable military missions at the speed and capacity required for modern conflict and ultimately lend to prosperity, security, and credible deterrence around the globe. Meeting the challenge will require breaking old molds and building new skill sets, partnerships, and ways of thinking.

Complicating the challenge, full-time career military members and their civilian counterparts typically do not have the expertise in global markets, financial services, acquisitions processes, and proficiency in statecraft and military strategy to engage effectively in economic statecraft planning or operations. Hence, identifying and nurturing such talent is an imperative that may require sourcing from uncommon areas where it does exist (and/or investing intentionally in the development of those skills). For example, certain individuals across the reserve components might possess the right expertise by having one foot in the civilian financial

services, corporate risk, or business intelligence sector and the other in military logistics, acquisitions, or counterintelligence.

Servicemembers should also be prepared to collaborate with America's partners and allies on economic statecraft activities, especially those with whom the United States shares significant economic and military ties. Operators should be able to recognize, comprehend, and address methods of economic warfare to safeguard shared supply chains essential to interoperability and core military missions, irrespective of the origin of the threat.

Working with private sector partners is equally vital for military and other national security professionals. Industry is fundamentally in the driver's seat when it comes to successfully addressing adversarial economics. Business leaders should be incentivized to proactively identify risk indicators within their industries and to educate their workforce on highlighting and mitigating economic-based risks to military missions. A successful economic statecraft campaign relies heavily on decisions and actions made by private sector actors, not just the government. Attuned to the situation or not, U.S. firms are crucial front-line actors in economic warfare.

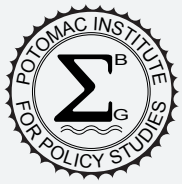
Economics has been weaponized on a global scale, driving it to be an active domain of statecraft with strategic, operational, and tactical dimensions. Durable partnerships should be mobilized between government and industry, at home and abroad, to secure technologies and supply chains critical to national security while preserving the values we aim to defend. America's greatest strength has always been its ability to innovate — to harness imagination and enterprise for the common good. That strength is still intact and should be directed with purpose. Economic warfare will be won by recognizing the battlefield for what it is, and by mobilizing the full spectrum of national power — economic, technological, and political — to secure our future prosperity and security.

Tim Welter, Ph.D., is a senior research fellow at the Potomac Institute for Policy Studies where he started and leads the Global Competition Project. Leveraging experience from Capitol Hill, the Pentagon, industry, and academia, his research is primarily focused on national security policy development and implementation, and economic statecraft.

The views expressed in this article reflects the author's personal thoughts and do not represent the position of the Department of the Air Force or the Department of Defense, with whom the author is also affiliated.

Margaret McWeeney, Ph.D., is a research analyst at the Potomac Institute for Policy Studies and International Center for Terrorism Studies. Her research focuses on hybrid warfare and nonstate actor security threats.

Economics is no longer just a lever of national power — it is an operational domain of warfare and economic statecraft provides an effective means to operate in that domain.



CHAPTER 1 EPILOGUE: MODELING THE THREAT, TESTING THE SYSTEM

Margaret McWeeney

"Sun Tzu in the Supply Chain" closed with a warning that economic warfare must be addressed by mobilizing the full spectrum of national power. What the article did not resolve is exactly how the United States organizes a cross-agency response to a threat this diffuse. This challenge is well recognized. The U.S. Government Accountability Office (GAO) has repeatedly identified difficulties in coordinating national security problems that cross agency jurisdictions, including gaps in overarching strategy, mechanisms for interagency action, and information sharing.[51] Additionally, Congress authorized the Countering Economic Coercion Task Force in the FY2023 NDAA with a mandate to develop an integrated U.S. strategy and facilitate coordination among federal agencies, but its effect has yet to be seen.[52]

Equally important, the private sector is squarely in the driver's seat when it comes to any strategy's successful address of adversarial economics. Cross-agency orchestration will require an innovative approach to how the government works with and integrates private-sector partners into strategy and practice. Properly tuned incentives will be at the center of a productive team effort, considering a balance of risks and rewards in decisionmaking, to train the workforce and give stockholders peace of mind. Decision calculus by U.S. firms in coordination with U.S. government entities will be crucial to success in economic statecraft.

This epilogue proposes a next step in aligning both fronts: a wargame designed to identify patterns in Chinese use of nonstate actors and rehearse a coordinated U.S. response before, rather than after, the next economic shock.

Modeling the Threat

The theft of intellectual property and subsequent capture of the commercial drone market is an illustration of adversarial economic statecraft, but it is one data point in a much wider and less orderly set of activities. China's toolkit reaches well past the market-capture sequence that produced firms like DJI.[53] Reporting alleges that China's nonstate actor threat also spans covert political influence run through the United Front Work Department,[54] cyber proxies with documented links to Chinese state and military organs,[55] Chinese dual-use technology reaching Houthi forces in the Red Sea,[56] and Chinese chemical manufacturers supplying the precursor chemicals that feed the cartel-run fentanyl trade into the United States.[57]

These cases differ substantially in actors, objectives, authorities, and attribution. Yet that is precisely the problem. They appear piecemeal in defense and congressional reporting, sanctions actions, intelligence assessments, and case-by-case prosecutions. Viewed together, however, they may reveal recurring methods for exploiting seams between U.S. economic, security, regulatory, and law-enforcement institutions.

Piloting an Economic Statecraft Wargame

Drawing on contemporary case studies, the pilot would adapt scenario-based wargaming to two related tasks: 1) identifying patterns in China's use of nonstate actors; and 2) testing the U.S. government's ability to respond across institutional boundaries.

The game begins with economic intelligence, or fused national-security and business intelligence, advocated by Karyn Eliot and Jennifer Buss in this series.[58] Participants would represent or bring experience from agencies including Defense, Justice, Homeland Security, Commerce, Treasury, and State. Rather than receive a fully formed description of the threat, they would encounter it incrementally, as officials would in practice.

For example, an opening inject might indicate that a nominally private Chinese company has begun acquiring or underpricing competitors in a strategically important U.S. technology market. A second could reveal previously unidentified state financing or ownership relationships. A third might introduce cyber activity against a U.S. competitor, acquisition of sensitive intellectual property, or transfers involving an intermediary in a third country. Later information could indicate that the technology has reached a sanctioned or hostile actor.

At each stage, the panel would have to decide: What do we know? What remains uncertain? Who owns the problem? Which authorities are available now, and what happens if the government waits?

Participants draw on a playbook of federal economic statecraft authorities explicated by William Norris in this series, identifying which office and department holds the relevant lever from export licensing and investment screening to sanctions, criminal prosecution, procurement restrictions, diplomatic engagement, and others.[59] The exercise would therefore test not simply whether the United States has adequate tools, but whether the agencies possessing them can recognize when they should be used and coordinate their application quickly enough to matter.

Successive rounds would complicate the decision. Attribution might remain uncertain. A proposed Commerce action could affect an ongoing Justice investigation. Treasury might possess a financial tool but lack sufficient evidence to deploy it. State might identify consequences for an ally whose cooperation is necessary to close the vulnerability. Industry could possess critical information that has not reached government analysts. The purpose is not only to manufacture an ideal response but to expose where information, authority, timing, and institutional responsibility diverge.

The principal output would be a decision matrix refined across successive games. For each threat pattern, the matrix would identify indicators and warning signs, relevant agencies and authorities, intelligence gaps, decision points, potential interagency conflicts, and pathways for escalation. Repeated games using different documented cases could reveal whether the same institutional seams recur across superficially different threats.

A Step Toward EWOC

The pilot would also serve as an initial test of the Economic Warfare Operations Capability (EWOC), a three-part structure combining observation and analysis of threats to the industrial base, durable government-industry partnerships, and an orchestration function capable of deciding, acting, or elevating when a threat requires it.[60] As Anita Kellogg argues in this series, a full EWOC should constitute a permanent capability within the Department of Defense or another agency.[61]

This pilot paves the way for one component of that larger concept: whether fused analysis of nonstate actor behavior can be translated into cross-agency action. A successful game would not demonstrate that the institutional problem has been solved. It would identify where the architecture breaks and what a permanent capability would need to repair.

A Note on The Adversary: The Intent Question

As in any wargame, the ability to anticipate the moves of the adversary is a powerful tool. In this case, however, the *why* and *how* behind China's use of nonstate actors and economic statecraft remain contested. It is tempting to read China's use of nonstate actors as a single coherent doctrine, but the scholarship does not support that certainty.

For instance, strategic-culture scholars root China's preference for indirect and asymmetric methods in ideas from the Thirty-Six Stratagems through Mao's theory of protracted "People's War."[62] International-relations scholars situate the same behavior in the structure of great-power competition, drawing on power-transition theory and the security dilemma to argue that a rising power has strong incentives to test and expand influence through deniable means rather than risk a premature confrontation with the incumbent power.[63] Also known as "lawfare" or "grey zone warfare," these theorists argue that China pursues a deliberate exploitation of gaps and weak enforcement in international law, from the law of the sea to cyberspace, that lets them operate in an ambiguous space below the threshold of armed conflict and without technically breaking rules.[64] More applied literature draws on principal–agent

theory from the study of state-sponsored proxies, arguing that states like China outsource the activities they would prefer not to be seen doing themselves, in patterns that vary with the nonstate actor's strength, targets, and transnational reach.[65]

These explanations need not be resolved before the United States can improve its response. The pilot instead begins with documented behavior. Participants receive cases with their context reconstructed and must determine what patterns they can defensibly infer and what actions those patterns justify.

Closing: Testing Ourselves, Not Just China

This series opened with Sun Tzu's maxim: know your enemy, know yourself. The proposed wargame tests both at once. It uses documented cases to improve understanding of how China employs nonstate actors while placing those patterns before the officials who would have to respond to them. The institutional gaps documented throughout this series can be tested in that room under the pressure of a live scenario.

The United States already possesses an extensive arsenal of economic statecraft authorities. The question is whether it can bring the right ones together at the right time. A pilot that exposes where the interagency system breaks down, and converts those lessons into a tested decision matrix, is a practical first step toward moving U.S. economic statecraft from reaction to prevention.

Margaret McWeeney, Ph.D., is a research analyst at the Potomac Institute for Policy Studies and International Center for Terrorism Studies. Her research focuses on hybrid warfare and nonstate actor security threats.

The United States already possesses an extensive arsenal of economic statecraft authorities. The question is whether it can bring the right ones together at the right time.



CHAPTER 2

ABSTRACT

No one entity actually orchestrates American economic statecraft. More than 1,400 offices across 13 departments and 10 federal agencies share relevant authorities, most of which sit dormant until the White House or a cabinet secretary orders them into action. Policymakers have traditionally organized the employment of economic statecraft around its tools. This article offers a framework built on the ends those tools serve, sorted into four kinds of activity: promote, protect, prevent, and punish.

Dr. Norris' recommendations begin with a proposed common definition of economic statecraft to be adopted across the U.S. government interagency to anchor doctrine and planning capabilities that do not exist today. He posits that universities should develop a professional pipeline able to staff and exercise those government activities while also preparing the private sector for success. Congress has its own reorganizing to do, and the article suggests either a new committee with requisite oversight authorities or a coordinating body for the chairs of existing ones.

Scan the QR code to view the webinar that accompanies Chapter 2.

Pierre Marshall/CC BY 4.0

ECONOMIC STATECRAFT AND THE FEDERAL INSTITUTIONAL ARCHITECTURE

William Norris

Who actually runs America's economic statecraft?

The answer matters because in today's great power competition, national security increasingly hinges on economic decisions made across a sprawling federal system — and often outside government altogether.

At its core, economic statecraft refers to the deliberate use of the government's economic policy tools and authorities to shape the behavior of commercial actors in ways that produce, mitigate, or manage national security externalities.[66] Firms, not states, are the actors conducting global economic activity. The consequences of their transactions — from investment to supply-chain structuring — often create strategic ripple effects. States can use government policy tools to intervene to align private incentives with national security priorities. This is the essence of contemporary economic statecraft.

What are the roles and responsibilities of the numerous U.S. government players involved in exercising economic statecraft authorities? This discussion about institutional architecture begins by offering a straightforward way to categorize the many authorities associated with economic statecraft. It then maps the landscape of key U.S. government players in this space before closing with several suggestions for how economic tools of national power can be used more effectively.

Traditionally, U.S. policymakers have understood and organized economic statecraft through the lens of the various tools in a toolkit, including sanctions, export controls, tariffs, development aid, and critical-infrastructure investment. But this is not a strategically coherent approach. The number of tools is almost infinite, and the relevant authorities are legion. A better way to organize this conceptual landscape is by the strategic ends that economic tools of national power can be used to pursue. This begins with adopting a common definition of economic statecraft that supports the development of doctrine. This adoption should transcend interagency boundaries. It can serve as the basis for improving cross-silo communication as well as building out planning capacity and analysis related to economic statecraft. A serious effort to improve how we conduct economic statecraft might also involve institutional and process redesign. Perhaps most significantly, we should invest in the human capital pipeline of talented individuals capable of operating effectively across both the private and public sectors. Our higher educational system needs to begin developing the skills and knowledge for a new generation of economic statecraft professionals. The way to begin is by clearly articulating the ends to which economic tools may be applied.

The Four P's of Economic Statecraft

The United States is a rule-of-law system and our economic statecraft institutional architecture reflects that transparent formality. When the government seeks to engage in economic statecraft, it acts through explicit "authorities": legislation, executive orders, statutes, or other legal and regulatory capacities that are often exercised by specific parts of the federal government.

Most of these authorities can be grouped into four kinds of activities:

Promote describes targeted manipulation of incentives facing firms and actors that has the effect of advancing the opportunities of U.S. companies, investors, institutions, etc.

Protect deals with government intervention designed to shield firms, industries, sectors, etc. from the market outcomes and commercial trends that have produced or may be producing outcomes that harm U.S. security. This includes measures traditionally considered "protectionist."

Prevent describes government actions that neutralize, block, remediate, or address acute (often discrete, specific) economic activities that threaten national security. This strategic effect is generally reactive and often involves specifically tailored measures (like Committee on Foreign Investment in the United States reviews).

Punish involves manipulating the economic levers designed to cause harm, reduce capacity, or undermine the target. Unlike the other three P's that often include an instrumental element to their strategic objectives, punishment seeks to inflict economic damage as an end in itself.

These four P's capture most of the ways the U.S. government conducts economic statecraft. Broadly adopting this framework and a private sector-centric approach to economic statecraft can help move the U.S. government toward an official, common operating picture.

Who's In Charge?

The current institutional landscape responsible for U.S. economic statecraft is sprawling. More than 1,400 offices spread across 13 departments, and 10 federal agencies share authorities and tools relevant to managing the economic dimensions of national security. This dispersion poses significant challenges. Agencies rely on legacy systems and approaches built for earlier eras and threat environments, reducing their ability to respond cohesively to today's challenges. Communication gaps between often siloed departments further complicates planning and implementation. There is a real need to develop a coherent interagency conceptual approach to economic statecraft that is doctrinally rigorous and includes planning and analysis capabilities that do not exist today.

The system tends to look upward for clear direction and instruction. Economic statecraft capabilities generally remain dormant until ordered into action by the White House or a proactive Department of the Treasury, State, Defense, or Commerce secretary. Although this passivity is somewhat understandable, the aggregate result is a tendency toward inertia and siloed economic statecraft in the face of myriad and complex challenges.

At the center of the U.S. government economic statecraft apparatus sits the Executive Office of the President that nominally coordinates cross-government economic statecraft activity through the National Security Council.[67] The National Security Council, however, is structurally inclined toward crisis response, limiting its ability to serve as a long-range integrator of economic statecraft. Other components within the Executive Office of the President — including the National Economic Council, the Office of Science and Technology Policy, the Office of the U.S. Trade Representative, the Office of Management and Budget, and the Office of the National Cyber Director — can also play significant roles frequently bringing distinct institutional perspectives into the process.[68]

Interagency integration of economic tools has typically been channeled through a hierarchy of Policy Coordinating Committees, Interagency Policy Committees, and their working subgroups and Deputies Committees.[69] These bodies often focus on specific issues or policy challenges, convening relevant departments when a decision or coordinated strategy is required. Yet even this structure tends to be reactive and fragmented rather than proactive, sustained, and strategic.

The Big Four (and Everyone Else)

Beyond the White House, there are four key departments that have typically been involved in leading various aspects of economic statecraft: the Departments of the Treasury, Defense, Commerce, and State. Improving information flows across these functional silos of economic statecraft would enhance the system's ability to coordinate and marshal the various capacities toward more unified strategic objectives.

Within the Department of the Treasury lie many of the government's most consequential economic statecraft authorities. Treasury houses the Office of Terrorism and Financial Intelligence, the Office of Foreign Assets Control, and the Financial Crimes Enforcement Network — agencies central to sanctions implementation, counter-illicit finance efforts, and financial-system security.[70] Other Treasury offices track international markets, development finance, and multilateral institutions. While Treasury plays an indispensable economic statecraft role, its institutional culture traditionally emphasizes macroeconomic stability and financial-system integrity rather than a strategic or security-driven mindset.[71] This can create dissonance when economic tools must be applied with geopolitical intent.

The Department of Defense represents another major player in economic statecraft. Although its authorities focus primarily on protecting defense missions and the defense industrial base, it brings advanced planning capacity, deep technical expertise, significant budgets, and a threat-oriented strategic culture. Key Defense entities include the Office of the Under Secretary of Defense for Policy, the Defense Advanced Research Projects Agency, the Defense Technology Security Administration, and the offices responsible for elements of research, engineering, and acquisitions.[72]

The Defense Department also has more explicitly economic statecraft-oriented components like the Office of Strategic Capital and the Office of Global Investment & Economic Security.[73] A future article in this series will focus on additional Defense Department concepts like the Economic Warfare Operations Capability and the Economic Defense Unit.[74] The Office of Global Investment and Economic Security evaluates national security risks associated with global transactions, serves as the Defense Department's point of contact for the interagency Committee on Foreign Investment in the United States, assesses mergers and acquisitions affecting defense supply chains, and develops mitigation strategies for transactions deemed risky.[75] It also participates in interagency bodies such as Team Telecom and contributes to antitrust reviews conducted by the Department of Justice and the Federal Trade Commission.[76] Beyond domestic responsibilities, the Office of Global Investment and Economic Security collaborates with U.S. allies to strengthen and coordinate industrial-base resilience efforts across partner countries.

The Department of Commerce also plays a central role in economic statecraft due to its control over export regulations, technology governance, and a host of other authorities. Its Bureau of Industry and Security administers export controls and maintains the Entity List, while the Export Enforcement Bureau and the Office of Export Enforcement investigate violations.[77] Additional Commerce components — such as the International Trade Administration, the Bureau of Economic Analysis, and the National Institute of Standards and Technology — contribute analytic capacity, standards leadership, commercial promotion, data aggregation, and regulatory tools.[78] Commerce wields many of the authorities central to technology-focused economic statecraft, though its traditional commercial-promotion culture can sometimes be in tension with the strategic imperatives of security-driven economic statecraft policy.

Finally, the State Department functions as a natural integrator across many dimensions of economic statecraft by virtue of its diplomatic role. Its Bureau of Economic and Business Affairs works globally to support U.S. companies, promote foreign investment into the United States, and deploy economic tools to constrain adversarial actors, including terrorists, corrupt officials, and human-rights abusers.[79] Embassy teams — including ambassadors, commercial officers, Treasury attachés, and State Department economic officers — engage directly with foreign governments and businesses, often serving as frontline practitioners of American economic statecraft.

An interesting innovation in State's approach to economic statecraft has been the deployment of Deal Teams, designed to mobilize interagency resources to support U.S. commercial competitiveness abroad.[80] These teams help U.S. firms compete in strategic sectors by coordinating feasibility studies, financing packages, technical assistance, and diplomatic engagement. Operating across posts worldwide and supported by a central Washington-based team, Deal Teams connect U.S. commercial activity with broader strategic objectives while leveraging the full interagency toolkit of the U.S. government.[81]

In addition to these "big four" economic statecraft departments and their associated offices, there are numerous other departments and agencies (e.g., the Federal Reserve, Department of Transportation, Export-Import Bank, Federal Communications Commission, National Science Foundation, Commodity Futures Trading Commission, Department of Agriculture, Federal Trade Commission, Department of Energy, etc.) that might also own more specialized components of the economic statecraft responsibilities.[82] Secondary and independent agencies can play substantial roles, but their contributions are rarely synchronized within a broader strategy.

Beyond these executive branch players, Congress acts as an important but structurally challenged participant. Legislative committees receive disparate information, and jurisdiction is splintered across multiple committees, complicating coherent oversight and strategic alignment. It is not clear that Congress is appropriately organized or institutionally prepared to effectively legislate on (or for oversight of) economic security challenges given its current jurisdictional committee lines.[83] Economic statecraft issues need a defined path for legislation, oversight, and funding that currently does not exist in Congress. An institutional change may be in order, either by standing up a new committee with the appropriate jurisdictional and oversight authority to address the transcendent nature of economic statecraft challenges, or by establishing a coordinating body for leaders of standing congressional committees with jurisdictional and oversight interests to raise, analyze, prioritize, and act on such matters. Contemporary economic statecraft is still quite nascent for the federal government. Much of this terrain is unprecedented. The practice of economic statecraft is likely to continue to be somewhat experimental. During this period of maturation, we should be flexible in our willingness to experiment and deliberate in our evaluation of what is working and what should be adjusted.

The institutional landscape of U.S. economic statecraft is highly fragmented. The authority to influence commercial behavior in support of national security is distributed across numerous departments — each with unique cultures, priorities, and processes. The challenge and opportunity ahead lie in forging a more coherent and strategically aligned system that can better coordinate tools, communicate priorities, and engage effectively with the private sector. We should innovate our government institutional design to facilitate more effective economic statecraft. As the economic dimensions of national security continue to expand — from technology competition to supply chain security to financial-system resilience — the need for integrated, modernized processes will only grow more urgent.

In addition to this institutional landscape, there are two high-profile standing interagency coordination processes that deserve attention: the Committee on Foreign Investment in the United States and the export control regime.

Committee on Foreign Investment in the United States

The Committee on Foreign Investment in the United States plays a central role in safeguarding U.S. national security by reviewing transactions that involve foreign investment or real estate acquisitions by foreign persons.[84] The committee operates as an interagency body chaired by the Department of the Treasury, which oversees these reviews through its Office of Investment Security.[85] Its core mandate is to identify and mitigate national security risks arising from foreign access to U.S. businesses, assets, technologies, or sensitive locations.

The Committee's authority derives primarily from Section 721 of the Defense Production Act of 1950, as amended, and is implemented through Executive Order 11858 and regulations detailed in Title 31 of the Code of Federal Regulations.[86] More recent presidential direction, including Executive Order 14083 issued in Sept. 2022, expanded and clarified the factors that the Committee on Foreign Investment in the United States considers, particularly in areas such as supply-chain security, sensitive data, and technological leadership.[87]

The committee's work depends on coordinated analysis by the Department of the Treasury, the Department of Defense, the Intelligence Community, the Department of Commerce, and other agencies. The Foreign Investment Risk Review Modernization Act of 2018 marked the most significant update to authorities in decades, broadening

jurisdiction to include certain non-controlling investments and specific real estate transactions.[88]

These efforts sought to modernize the process in response to emerging risks, but challenges remain. For example, the committee acts preventatively but only on a case-by-case basis, making it difficult to keep pace with the quantity of rapidly evolving foreign-investment threats. The system's reactive and bespoke approach can get overwhelmed and can miss activities, prompting calls for mechanisms to more easily clear benign and block clearly illegitimate transactions.[89]

Export Controls

Export controls govern the transfer of specific items, technologies, and services that may pose national security risks if provided to certain actors or destinations. The process begins with identifying an item's technical attributes and intended use, then classifying it under the appropriate Export Control Classification Number within the Commerce Control List, which determines the level of control required.[90]

The Export Administration Regulations cover dual-use, commercial, and less-sensitive military items.[91] Even low-tech goods may require licensing depending on the destination, end user, or end use. The Bureau of Industry and Security evaluates four key factors to determine license requirements: what is being exported, where it is going, who will receive it, and how it will be used.[92]

Effective export-control administration requires extensive interagency coordination led by the Department of Commerce and involving the Departments of Defense, State, Treasury; intelligence agencies; and others. Export controls were initially designed during the Cold War to prevent the transfer of military technology to adversary nations. The expanded application of export controls in the semiconductor realm as part of a larger effort to hamstring China's technological prowess and maintain U.S. leadership over key dual-use technologies of the future has strained existing institutions like the Export Control Review Committee.[93] We are trying to do a lot of economic statecraft using interagency institutional coordinating mechanisms that do not scale well.

Where We Go from Here

As we seek to enhance and leverage American economic power, we should do so in a way that is politically and economically durable and redounds to our considerable natural strengths. We also should be humble and realistic as we try new efforts to improve economic statecraft. Much of this is uncharted waters for the United States.

William Norris, Ph.D., is director of the economic statecraft program and an associate professor at the Bush School of Government and Public Service at Texas A&M University.

Economic statecraft issues need a defined path for legislation, oversight, and funding that currently does not exist in Congress.

CHAPTER 2 EPILOGUE: DESIGNING INSTITUTIONS FOR ECONOMIC STATECRAFT

William Norris

The current international environment presents the United States with several uncomfortable strategic realities. The nature of the challenge that the United States faces demands a response. Even if our system of government and our system of economic organization may ordinarily prefer not to link economic activities with national security, adversarial nations like Russia and China do. Under those circumstances, if we choose not to act, we do so at our own peril. But any sort of economic statecraft is necessarily going to be a market distortion. Typically, market distortions quickly become inefficient over the longer time scale and can lead to rent-seeking behavior, lobbying, further subsidies, and other downstream and upstream market distortions. Since economic statecraft is not something that the United States is all that well designed to do (nor is it necessarily part of our national DNA to mess with markets), we must design with humility.

As we seek to reorganize U.S. governmental capacity in the economic statecraft arena, we should build institutions that can fail gracefully (rather than catastrophically) if something does not go as intended. When we experiment, we ought to recognize the uncertain nature of this endeavor and design for safe fallback options. We should deliberately revisit our key assumptions in light of additional evidence and build in the capacity to objectively evaluate how our efforts to innovate have fared. Part of this experimental voyage should incorporate explicit organizational evaluation capacity to assess performance and detect when and why developments are not meeting expectations. We ought to pre-plan explicit stock-taking mechanisms to do this sort of self-analysis, benchmarking, and external evaluation to iteratively hone our institutional reform efforts in the economic statecraft domain.

Ideally, we can find ways to harness our natural competitive dynamics (e.g., partisan motivations to point out faults in the other party's efforts; inter-bureaucratic rivalries for missions, jurisdictional turf, personnel, and budgets; legislative-executive branch tensions; commercial competitors' tendency to fight for market share, etc.) to help constructively provide the most critical eyes on various economic statecraft initiatives. By leveraging these kinds of naturally occurring competitive tendencies, we can ensure that the most incentivized critics can help sharpen the overall tendency of the system toward increasingly effective activities, structures, processes, and organizations. Over time, such dynamics would help produce improved economic statecraft from the United States.

Principles to Guide the Design and Practice of American Economic Statecraft

All strategies rest on principles or assumptions that guide them. Below are seven principles derived from our unique strengths and assets as a nation.

1. As a general rule, we ought to design economic statecraft in light of the commercial incentives that drive the private sector. Use government policy to work with and harness these interests by incentivizing them — rather than trying to fight against this grain or trying to wish them away. Successful economic statecraft must operate through incentives to shape and leverage the scale, ingenuity, and vibrancy of American enterprise. Success will require working with the American private sector, not against it.

2. Our national power ultimately derives from U.S. economic growth and innovation. Increasing long-run productivity gains is key to succeeding in any international competition. Real gains in productivity come from innovation. Our sustained capacity for radical innovation is the key competitive advantage for the U.S. Such innovation can completely change the "rules of

the game" with a new way of doing things, novel technologies, or sometimes entire industries that result. This kind of creative destruction is a hallmark of our adaptable, entrepreneurial, free-market system. The pillars of our innovation system — including world-class higher education, our research ecosystem, legal infrastructure, markets, data, human capital — ought to be deliberately fostered, preserved, sustained, and shielded from deliberate efforts to undermine them.

3. When it comes to designing industrial policy, we must be constantly on guard against "capture." Our political system (especially when it interacts with business) is prone to what social scientists call "capture," which means that groups with fairly narrow agendas and preferences will tend to dedicate resources and efforts to lobby Congress to advance their narrow interests whether or not that is actually in the nation's best interest. We need, therefore, to be very careful about industrial policy, protectionism, or other sorts of market-distorting measures as these can easily lead to inefficiencies and a failure to innovate.

4. The U.S. should have a preference to rely on market-oriented solutions since those tend to be most efficient and sustainable over the long term. Government initiatives are most effective when they are focused on addressing market failures.

5. U.S. economic statecraft should maximize scale and legitimacy by coordinating and leveraging the power of allies and partners. Such aggregation would provide scale for markets that would help drive innovation and offset the draw of China's large internal market. This strategic aggregation of leading nations is an unmatched, and sustainable comparative advantage for the United States.

6. The U.S. enjoys a big "incumbency advantage" in any long-term competition. The United States wrote the rules of today's voluntary, open, transparent, and improvable global economic order. We are, as a consequence, the dominant nation in global affairs. Although we face rising challengers, we should force those challengers to make the case for why things would be better when they get to write new rules for international commerce. By deliberately forcing challengers to justify any changes, we also call attention to the inherent benefits of the current order and its improvability.

7. As we move forward in the economic statecraft domain, it is crucial to focus on the various ways that government and diplomacy can support different kinds of business, investment, and trade to help create jobs for Americans and new opportunities for American businesses. America has always stood for the advance of equality and liberty, but it will be impossible to realize these noble aims at home or internationally if the underpinning economic success is not in place to support them.

William Norris, Ph.D., is director of the economic statecraft program and an associate professor at the Bush School of Government and Public Service at Texas A&M University.

Even if our system of government and our system of economic organization may ordinarily prefer not to link economic activities with national security, adversarial nations like Russia and China do.

CHAPTER 3

ABSTRACT

Enduring economic security must rest on more than goodwill and occasional exchange of personnel between the public and private sectors. Drawing on Eliot's experience in the intelligence community and the boardroom, the authors make the case for fusing national security intelligence with business intelligence as a sustained discipline. This means something narrower than sharing classified reporting: a standing analytic practice that distills what the government knows into sector-level warnings companies can act on.

Their central recommendation is a dedicated economic intelligence integration function, jointly staffed by the intelligence community, the Departments of the Treasury and Commerce, and private-sector detailees. Such a function would move the country beyond case-by-case transaction review and toward catching strategic patterns while there is still time to act.

Scan the QR code to view the webinar that accompanies Chapter 3.

Pierre Marshall/CC BY 4.0

FIGHTING AN ECONOMIC WAR WITHOUT FUSED INTELLIGENCE

Karyn Eliot and Jennifer Buss

In a corporate boardroom reviewing a high-stakes multinational deal, every financial risk was dissected — but no one in the room could see the classified intelligence that might have changed the decision entirely.

Right now, the United States is fighting an economic war without organizing itself for one.

While adversaries deliberately weaponize supply chains, capital flows, technology access, and industrial dependencies, the United States continues to operate its economic and national security systems along largely separate lines — managed through distinct authorities, processes, and intelligence channels. The result is a structural information gap between what the government knows and what private-sector decision-makers need to know. Closing that gap requires integrating national security intelligence with business intelligence in a disciplined, continuous way — before vulnerabilities harden into strategic disadvantage.

I first began to understand the depth of this problem while still in government. Intelligence reporting was increasingly clear about how competitors were using capital, supply chains, and commercial access to shape strategic outcomes. Yet there was no corresponding architecture to translate those insights into coordinated economic action. Authorities were dispersed. Jurisdictions overlapped. Intelligence was collected for national security purposes, but the companies making consequential economic decisions rarely had visibility into the risks identified by the government.

The gap was structural, not personal. It was not a failure of expertise. Rather, it was a failure of integration. In internal discussions, we could map adversarial behavior with precision — yet there was no parallel mechanism to inform the companies whose decisions were shaping the same strategic terrain.

The military trains to make choices in the field with incomplete information, to assess risk under uncertainty, and to act anyway, because waiting for perfect clarity is often the most dangerous choice available. My transition from government to the private sector exposed this as a gap in corporate decision making, both in boardrooms and throughout executive management. Working with companies, investors, boards, and technology firms, whose decisions sit directly on the front lines of a contested economic landscape, made it clear that the problem is not a lack of sophistication in mitigating the risks — it is a lack of visibility. Decisions with national security implications are made in boardrooms every day without access to the information that would fundamentally change the risk calculation. The government collects this information, called intelligence, and cannot reasonably share it with the companies that need it most.

The new *National Security Strategy* recognizes that economic security is fundamental to national security, but the government still operates systems as if they are separate.[94] Fragmented authorities, siloed information, and no mechanism for fusing intelligence lead to increased risk and poor decisions. Treating business intelligence and national intelligence as distinct has created blind spots

that adversaries are far more willing, and far more able, to exploit. It is critical to fuse U.S. intelligence community acumen with the private-sector knowledge to create action-oriented insights and mitigation plans.

Sharing Expertise

For years, government engagement with the private sector focused primarily on established defense contractors and technology vendors. That model reflected an era when national security risk was concentrated in traditional defense supply chains. Today, many of the most consequential decisions shaping strategic advantage are made by venture capital firms, private equity funds, institutional investors, and other capital allocators whose decisions determine which technologies scale, which firms survive, and which markets consolidate.

Government engagement with these communities expanded accordingly. Officials sought to understand how risk is assessed, how uncertainty is priced, and how investment committees make decisions under time pressure. In some cases, engagement moved beyond dialogue. Government personnel were placed on structured rotations inside venture funds and investment firms for defined periods not to influence outcomes, but to observe and learn. Those individuals gained direct exposure to how incentives drive capital allocation, how speed alters risk tolerance, and how competitive markets reward early positioning. In those settings, I watched investment committees debate risk in real time. Their speed and adaptability to adjust assumptions within hours as new information surfaced was striking. By contrast, government analytic processes were often optimized for deliberation rather than immediacy. The difference was not about competence, but about structure.

These personnel exchanges were valuable. They improved mutual understanding and clarified institutional constraints. But they also revealed a deeper problem: Insight without integration does not change outcomes.

Even when relationships are strong, national security intelligence remains confined to classified channels, and market intelligence remains proprietary and commercially guarded. Each side improves its understanding of the other, yet neither gains a fused picture of how adversarial intent, capital deployment, technology development, and supply-chain positioning intersect in real time.

The question is not limited to my experience in the boardroom. In 2020, Intel decided to outsource leading-edge fabrication to Taiwan Semiconductor Manufacturing Company following delays in its internal process development.[95] From a commercial perspective, the decision was rational — grounded in competitiveness, speed, and market positioning. But it raises a broader structural question: Would that calculation have been different if corporate leadership had access to the same insight the U.S. intelligence community had regarding Taiwan's vulnerability, semiconductor concentration risk, and long-term leverage dynamics?

As long as engagement remains relational rather than structural, the system continues to rely on informal awareness rather than institutionalized synthesis. That may reduce friction but it does not close the information gap.

If economic security is to mature as a strategic discipline, integration cannot depend on periodic exchanges or goodwill. It should be embedded into analytic architecture.

The Risk of Inaction

Government institutions are well-practiced at identifying the risks associated with action: legal exposure, political consequences, compliance missteps, and reputational damage, to name a few. These risks are visible, measurable, and tied to discrete decisions. They are documented in memoranda and reviewed in oversight hearings.

The risks of inaction are different. They rarely trigger immediate consequences. They accumulate. I have sat in meetings where action was deferred because no single agency owned the full picture. Each stakeholder saw part of the risk. No one saw enough to compel decisive movement. The absence of integration made delay appear prudent.

In economic security, inaction does not mean doing nothing. It means allowing fragmented systems to operate without integration. It means observing capital flows as they reshape strategic sectors

without pattern-level analysis. It means treating individual transactions as isolated events rather than components of a broader positioning strategy.

The costs surface slowly — in hardened supply-chain dependencies, in technology ecosystems that scale under alternative governance models, in minority investments that aggregate into influence, and in leverage that becomes apparent only after it has matured. By the time a vulnerability is visible within a single transaction, the pattern that created it is already well established.

Adversaries exploit precisely this gap between formation and recognition. In cybersecurity, we call this a zero-day vulnerability — a weakness that exists before defenses are calibrated to detect it. Economic vulnerabilities function similarly when intelligence and market data remain siloed.

The absence of integration is itself a risk multiplier. Without a sustained mechanism for fusing national security intelligence and business intelligence, decision-makers on both sides act within incomplete frameworks. Markets optimize for return. Government optimizes for compliance and statutory mandate. Neither sees the full strategic picture.

In a contested economic environment, that structural separation compounds over time. Economic security cannot rely on reactive correction. It requires anticipatory integration.

Due Diligence Without the Full Picture

Firms and investors conduct rigorous due diligence to mitigate risk based on many factors

including examining financials, regulatory compliance, and market projections, but often without visibility into international and geopolitical dynamics. Due diligence is undermined when national security intelligence and private-sector business intelligence remain siloed. Nuanced insight from the national security enterprise for national purposes would perhaps shift corporate decisions. Additional risks could be factored into their calculations resulting in a more robust analysis.

During an executive meeting evaluating a cross-border technology merger, I watched a board conduct exhaustive financial and regulatory due diligence. Yet no one in the room was factoring adversarial capital influence, opaque state-linked investors, or downstream supply-chain dependencies. The transaction was compliant. It was profitable. It was rational. It was also strategically risky in ways invisible to those without access to national security intelligence.

The individuals in that room were neither careless nor uninformed. The gap was structural. The information that would have materially changed the risk calculus existed inside government systems. The process is not designed to inform private-sector decision-making, let alone doing it in real time.

In the private sector, market intelligence is a competitive asset and treated as confidential company information. Corporate engagement with government in any form is associated with regulatory exposure (high risk). Within the U.S. intelligence community, the same posture is true, but for different reasons. The intelligence community protects sources and methods which makes sharing information with industry inherently risky and less credible. These stances are understandable, yet together in the ecosystem they shatter the trust required for sustained collaboration because neither side sees enough return to justify the exposure.

Neither the U.S. government nor corporate America captures all the risks in their respective analyses, and it is not because their work is careless. Both sides operate with incomplete information. Deliberately fusing that information in near-real time would enhance our security and help safeguard our economy. Patterns only emerge when the data is integrated.

Why Existing Approaches Fall Short

Existing approaches to economic security fall short not because of lack of effort, but because they remain fragmented and largely transaction driven. The structure of the U.S. federal departments prevents sustained integration. Here we explore a few examples to highlight the disconnects across increasing hierarchy: committees, departments, communities, and strategic programs.

The interagency Committee on Foreign Investment in the United States reviews foreign investment transactions and has expanded its authorities

considerably in recent years, including under the Foreign Investment Risk Review Modernization Act of 2018.[96] Yet the committee is inherently transaction-bound. Its mandate is to assess specific deals that are formally presented for review. In practice, that means analysis begins only once a transaction is visible. By the time a deal is filed, much of the strategic positioning may already be complete. It does not monitor broader capital flows across markets, nor was it designed to identify emerging patterns of strategic investment before leverage materializes. As a result, the mechanism functions as a gatekeeper, not as a sensing platform.

Consider minority investments in emerging technology firms. Individually, these stakes often fall below formal review thresholds and present no immediate national security trigger. The deals are structured to be non-controlling, compliant, and commercially routine. Collectively, however, they can provide technical and intellectual visibility, information access, supply-chain positioning, and long-term influence across an entire sector. No single transaction appears malicious. The accumulation of these investment deals reveals a pattern of strategic behavior. By the time influence is visible through a single transaction, the strategic posture is mature. Transaction-level review mechanisms will not detect pattern formation.

Federal departments with deep economic expertise, including the Department of the Treasury, Commerce, and State, collect and analyze substantial financial and commercial data. However, they are organized to serve their statutory missions, not to synthesize those insights into forward-looking national security assessments for private-sector decision-makers. No single institution is responsible for assembling a comprehensive picture of how capital deployment, technology transfer, and supply-chain positioning intersect strategically.

The intelligence community, for its part, excels at identifying adversarial intent, sanctions evasion, and covert financial networks. It is less structured to evaluate how adversaries use lawful capital investment, minority stakes, joint ventures, and commercial partnerships to advance long-term strategic objectives. Those activities often fall below traditional intelligence warning thresholds. Meanwhile, various offices across government, including the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, and the Pentagon's Office of Strategic Capital, provide valuable briefings and partnership initiatives. These efforts improve awareness. But awareness alone does not constitute integration. Information is shared in discrete engagements rather than synthesized into a sustained analytic framework to shape capital allocation and board-level decisions.

The result is not absence of action. It is absence of architecture.

What Fusion Actually Means

Fusing national security intelligence with business intelligence does not mean broadly sharing classified reporting or turning companies into extensions of the intelligence community. That framing has slowed serious discussion by conflating purposeful integration with unnecessary exposure.

In practice, fusion is disciplined and practical. Fusion means translating intelligence-derived patterns into sector-level risk indicators that can be shared responsibly. It means moving beyond transaction review toward strategic sensing. It means identifying how adversarial capital deployment, technology positioning, supply-chain concentration, and market consolidation interact over time.

Fusion is not firm-specific targeting. It is structured synthesis.

Information should move in both directions. Industry insight, such as market behavior, emerging technologies, pricing signals, and supply constraints, strengthens government analysis. National security intelligence, such as adversarial intent, covert financing patterns, and long-term strategic positioning, strengthens corporate risk assessment. The objective is not data exchange for its own sake. It is decision support. When intelligence informs operational decisions in government, outcomes improve measurably. Economic decision-making deserves the same analytic rigor.

There is precedent for this. Civil-military cooperation in cybersecurity evolved from *ad hoc* briefings

into structured mechanisms for rapid information exchange and coordinated response. Economic security requires a similar maturation — one that embeds integration into analytic architecture rather than relying on periodic outreach.

Done well, fusion informs capital allocation, supply-chain design, technology partnerships, and foreign investment decisions before vulnerabilities harden into adversarial advantage. It allows leaders to see patterns rather than isolated events.

Integration does not eliminate risk. It reduces blind spots.

What Should Change

Economic security will not mature through episodic engagement or expanded transaction reviews alone. Structural integration is required. Three changes are essential.

First, establish a dedicated economic intelligence integration function staffed jointly by intelligence professionals, Treasury and Commerce analysts, and detailees with private-sector expertise to synthesize national security intelligence and commercial data into sector-level risk assessments. No single organization currently assembles this picture.

Second, shift from transaction review to pattern detection. Mechanisms like the Committee on Foreign Investment in the United States are reactive and transaction-bound. Intelligence integration for economic security requires identifying strategic investment trends and dependency formation before leverage is exercised.

Third, identify and share the risk indicators of economic security to inform decision-making. We should normalize sector-level intelligence products for boards and investors.

A More Secure Way Forward

Economic security comes with clear articulation of risks, dependencies, and tradeoffs. Economic intelligence is an asset in decision support, not merely for alerting officials.

Addressing the information-sharing problem does not require dismantling existing legal frameworks or compromising civil liberties. It does not require broader sharing of sources or methods that may compromise intelligence-gathering activities. It simply requires more intentional use of the authorities and discretion already available. Analysts and policymakers should continue to investigate carefully and lawfully with fusion approaches to bring together national security intelligence, economic data, and commercial insight.

Decision-makers act within their respective authorities. Sharing intelligence to inform those decisions is in the best interest of the private sector and the national security enterprise. Fusing private and public sector data empowers leaders to make informed decisions about the future of the United States.

Public-private engagement, particularly with capital investors, is an ongoing learning opportunity for both sides. Government has much to learn about how risk is priced from the commercial perspective and how uncertainty is managed in any number of scenarios and markets. At the same time, public judgment, accountability, and strategic perspective remain essential correctives to purely market-driven outcomes. The federal government has the responsibility to make it easier to share decision-relevant insights with the private sector decision-makers who need it most. Excessive caution driven by fear of missteps can be as damaging as recklessness and inaction.

Finally, economic intelligence as a domain requires professionalization. Analysts and leaders who understand both markets and security, operating under clear doctrine and oversight, are essential if economic security is to mature beyond a collection of well-meaning initiatives.

Conclusion

Economic security and national security are mutually reinforcing. Ignoring that reality does not preserve values or reduce risk. It shifts risk into places the United States is less prepared to measure and mitigate. The greatest danger is not flawed

engagement between government and industry. It is the institutional comfort of fragmentation.

Economic security cannot remain a collection of well-meaning initiatives. It should become a professionalized discipline with clear doctrine, integrated intelligence, and defined responsibility.

The United States has the tools. What it lacks is integration. In a contested economic environment, that gap is not theoretical — it is a strategic vulnerability.

The structural separation addressed here is primarily domestic. Yet adversarial systems do not operate with similar distinctions between commercial and state actors. In some models, civil and military capabilities are deliberately integrated in ways that amplify economic leverage. Understanding how that integration functions across borders — and how democratic systems can respond without compromising their own legal principles — is the next dimension of economic security and the focus of the next article in the series.

Karyn Eliot is a retired senior CIA executive with more than two decades of experience in intelligence leadership, interagency coordination, commercial partnerships, and allied engagement. She now works at the nexus of national security and economic decision-making, including as a strategic account executive at Rohirrim and as a partner at Five Eyes Group.

Jennifer Buss, Ph.D., is the chief executive officer of the Potomac Institute for Policy Studies. She has worked across industry and government facilitating information sharing to advance national security.

In economic security, inaction does not mean doing nothing.
It means allowing fragmented systems to operate without integration.

CHAPTER 3 EPILOGUE: THE NEXT CHAPTER OF ECONOMIC STATECRAFT — FROM INFORMATION FUSION TO DECISION ADVANTAGE

Karyn Eliot

When "Fighting an Economic War Without Fused Intelligence" was published, the central argument was that the United States faced an information problem — not because it lacked intelligence or commercial insight, but because it lacked enduring mechanisms to integrate them into strategic decision-making.

I believe that argument remains as relevant today as when the article first appeared. What has changed is the conversation itself. Economic statecraft has moved beyond recognizing the need for greater collaboration between government and the private sector. The discussion is now focused on implementation: how democratic nations can build trusted, practical mechanisms that transform information into action while preserving the legal authorities, commercial incentives, and democratic values that distinguish them from strategic competitors.

Much of my career has been spent translating between worlds that often see the same problem through very different lenses — first in the intelligence community and later working with companies navigating an increasingly complex geopolitical and economic landscape. That experience has convinced me that our greatest barriers are rarely technical. More often, they are institutional, cultural, and simply the absence of sustained relationships.

During my years in government, I came to appreciate that our greatest challenge was rarely collecting information. The United States is exceptionally good at that. The harder problem has always been connecting insights generated by government, industry, finance, academia, and allied partners before critical decisions have to be made.

One lesson I carried with me from government into the private sector was how often different organizations were observing the same emerging problem from entirely different vantage points. Intelligence analysts might recognize geopolitical intent while companies noticed unusual supplier behavior, investment decisions, or shifts in customer demand. Each observation was accurate, but neither told the whole story. It was only when those perspectives were considered together that the broader strategic picture emerged. That experience reinforced for me that our greatest challenge has never been collecting more information. It has been creating the relationships and mechanisms that allow us to connect what we already know before important decisions have to be made.

The debate has evolved. The question is no longer whether government and industry should work together more closely. They already do. The real question is how to build enduring institutions and trusted relationships that allow each to contribute what the other cannot. The next phase of economic statecraft is not about collecting more information. It is about creating Decision Advantage.

Information Alone Is No Longer Enough

Government understands strategic intent. Industry understands markets, investment, innovation, technology, and execution. Financial institutions see patterns of capital and risk. Academia often identifies emerging trends before they become widely recognized. Each perspective is valuable. None is sufficient on its own.

In my experience, the most consequential decisions were rarely made because someone possessed more information. They were made because the right people were able to combine different perspectives before opportunities were lost or emerging risks became far more difficult to manage. That ability to connect people and ideas across institutional boundaries is ultimately more valuable than simply collecting more data.

Meanwhile, our competitors are already integrating economic, technological, financial, and industrial tools in ways that blur the line between commercial competition and national strategy. Democratic

nations should become much more deliberate about connecting our own strengths while preserving the openness and innovation that make them possible. Collecting information has never been America's greatest challenge. Turning shared understanding into timely decisions has been.

From Information Fusion to Decision Fusion

The original article argued that government intelligence and commercial intelligence should be fused to produce a more complete understanding of strategic risk. I continue to believe that is essential, but information itself is not the objective. Information creates value only when it improves decisions.

The next evolution of economic statecraft should therefore focus on Decision Fusion — bringing together intelligence assessments, commercial insight, financial analysis, industrial capacity, technological expertise, and allied perspectives so leaders can make better decisions, faster and with greater confidence. Information sharing is an activity. Decision Advantage is the outcome.

Strategic Signaling Matters

One thing I've come to appreciate since moving into the private sector is how differently government and business experience uncertainty. Governments often respond to rapidly changing events. Companies make investment decisions that shape their businesses for decades.

Clear strategic direction often matters more than detailed prescription. It gives industry the confidence to make long-term investments, strengthen supply chains, pursue innovation, and align with national priorities while preserving the flexibility and dynamism that only free markets can provide. Government and industry each have distinct roles to play. Economic statecraft is most effective when those roles are understood, respected, and mutually reinforcing.

Technology Changes the Scale — Not the Challenge

Technology — including artificial intelligence — will dramatically improve the speed at which governments and companies collect, process, and analyze information. But speed alone does not produce better decisions. Human judgment, trusted relationships, and effective institutions remain indispensable. Technology can accelerate good decisions, but it cannot replace the people, partnerships, and governance that make those decisions possible.

Allies Multiply Our Competitive Advantage

No democratic nation possesses every critical technology, every strategic resource, or every industrial capability. One of our greatest advantages has always been our network of allies and partners. The more effectively we connect complementary strengths across trusted nations, the stronger our collective resilience and our ability to compete.

The Private Sector Is a Strategic Partner

Companies are no longer simply stakeholders affected by national security policy. They increasingly shape it through innovation, investment, infrastructure, and supply chains. Government and industry are solving different parts of the same problem. Neither perspective is complete on its own, and neither succeeds without the other.

Looking Forward

The conversation surrounding economic statecraft has matured considerably since the original article was written. We have spent much of the past several years defining the challenge. The next phase must focus on implementation.

One thing I've learned over the course of my career is that collaboration isn't something you can surge during a crisis. Trust takes years to build and only moments to test. The relationships that matter most are almost always established long before they're needed.

The United States begins from a position of enormous strength. Our intelligence capabilities, innovative companies, research institutions, capital markets, and alliances remain unmatched. The opportunity before us is not to create entirely new capabilities, but to connect the remarkable strengths we already possess.

The work ahead is less about inventing new strategies than building stronger relationships and trusted mechanisms that turn shared understanding into timely action. We have no shortage of good ideas. The opportunity now is to move beyond discussion and put those ideas into practice — before crises force us to.

If economic statecraft is to become a lasting competitive advantage, it will not be because we collected more information. It will be because we learned to make better decisions together.

Karyn Eliot is a retired senior CIA executive with more than two decades of experience in intelligence leadership, interagency coordination, commercial partnerships, and allied engagement. She now works at the nexus of national security and economic decision-making, including as a strategic account executive at Rohirrim and as a partner at Five Eyes Group.

The work ahead is less about inventing new strategies than building stronger relationships and trusted mechanisms that turn shared understanding into timely action.

CHAPTER 4

ABSTRACT

The contest over critical industries will be decided by whoever organizes capital quickly and deliberately. Heavily consequential industries, from advanced manufacturing to the infrastructure behind generative AI, sit on private balance sheets and in global supply chains, at a scale government budgets would be hard-pressed to match. A new generation of investment vehicles has emerged in response, using public money to absorb early risk and pull private capital toward strategic sectors. These experiments remain small and scattered relative to the task.

Skipper's recommendations start with allies agreeing on a shared list of priority projects and aggregating demand across borders so that major investments become commercially viable. From there, the article proposes an Indo-Pacific critical industries fund anchored by the United States, Japan, and Australia and drawing on the region's deep pension capital. With trust in China's Belt and Road Initiative eroding, there is an opening for allied financing that operates on open terms.

Scan the QR code to view the webinar that accompanies Chapter 4.

Pierre Marshall/CC BY 2.0

FOLLOW THE MONEY: FINANCE AND THE FUTURE OF ALLIED ECONOMIC STATECRAFT

Georgie Skipper

What if the real battlefield of great-power competition is the global flow of money?

The ability to mobilize and direct large pools of public and private capital across critical industries — defense, infrastructure, manufacturing, and technology — is becoming the defining instrument of contemporary economic statecraft. These industries operate largely in private balance sheets and global supply chains, meaning governments should increasingly align national priorities with private investment.

As a result, a new toolkit of economic statecraft is emerging. Governments are turning to investment vehicles, financing platforms, and policy incentives that bring public priorities and private capital closer together.

Contemporary economic statecraft now operates across three interconnected layers: finance, the physical infrastructure that enables industry, and the technology that sits on top of that infrastructure.

This article examines why the capital intensity of critical industries is forcing a deeper relationship between governments and private markets. It uses the generative AI infrastructure boom as a short case study before exploring how finance is emerging as the central instrument of economic statecraft. It concludes with practical recommendations for the United States and its allies — from lowering the cost of capital and signaling priority projects, to aggregating allied demand, building new financing platforms, and accounting for strategic economic value.

AI Infrastructure: Finance, Friends, and Physical Assets

The generative AI infrastructure boom illustrates how the layers of finance, physical infrastructure, and technology interact in practice. Critical industries are capital-intensive and often require patient capital over long investment cycles, in multiple geographies. The generative AI boom has accelerated the demand for the physical infrastructure that enables these industries, including power generation, data centers, digital connectivity, and critical minerals.

Energy supply has become the central constraint. According to Nvidia's CEO, the cost of a one-gigawatt AI data center is immense.[97] While the exact amount varies, it is thought to be approximately $35–60 billion.[98] No single country controls all these inputs, which means the infrastructure behind AI is inherently global. Many countries with these required inputs are emerging markets. In the Indo-Pacific, the region's data center market is forecast to grow to $53.58 billion by 2028, with the Bank of America identifying a potential multi-year run driven by AI-related commodity and energy demand in emerging markets.[99]

The implication is clear: the countries that organize capital, energy supply, and infrastructure fastest will shape where the AI economy ultimately scales and who gains from the value creation. For the United States and its allies, the strategic task is not simply technological leadership but ensuring

that the finance, physical assets, and supply chains needed to support that technology are built within trusted economic networks.

New Financial Vehicles, New Statecraft

Finance is becoming the central mechanism through which allies and partners coordinate on critical industries, as governments deploy investment vehicles, financing platforms, and policy signals to reduce early risk and crowd private capital into strategic sectors. Initial models are already emerging across the United States and allied economies, largely focused on venture-scale investments in technology and dual-use capabilities, with some signs of critical industry coordination.

The U.S. Department of Defense Office of Strategic Capital, established in 2022, currently deploys approximately $1.2 billion through direct loans of up to $150 million per project and up to $175 million in fund financing.[100] The United Kingdom's National Security Strategic Investment Fund, launched in 2018 with the British Business Bank, co-invests alongside commercial funds, provides market intelligence, and helps firms navigate government procurement.[101] Its capital base is modest, but its proximity to demand gives it influence.

Australia's newly announced venture-backed defense vehicle adds another model.[102] With up to $350 million targeting cyber, AI, quantum, electronic warfare, and undersea systems, it aims to crowd private capital into sovereign capability. Its success will depend on quickly partnering with private industry and ensuring funded companies have sufficient defense and allied customers to remain commercially viable.

At the multinational level, the NATO Innovation Fund sets the highest benchmark for regional capital aggregation and investments.[103] Launched in 2022 with approximately $1.2 billion from 24 allies, it is the first multi-sovereign venture fund of its kind.

These investment vehicles share core features.[104] They deploy public capital as debt or equity to crowd in private investment and absorb early-stage risk. They limit where the money can come from and where it can be invested, keeping it mainly at home to strengthen national capacity, and in some cases, allowing it to flow only to trusted partner countries. Their effectiveness depends on clear investment mandates, strong investment opportunities, and the ability to translate government needs into commercial terms or private sector innovation into dual-use applications.

While these vehicles are useful, they also face limits. Government balance sheets are finite. Risk tolerance is often low. Australia's National Reconstruction Fund illustrates the growing pains common to this emerging asset class: navigating the tension between institutional risk culture and a bold policy mandate, slow early deployment, and the political scrutiny that comes with deploying public capital.[105]

Finance is becoming a central component of how allies and partners coordinate on economic statecraft. Public money is being used to set direction and lower early risk, and private capital is moving in where returns are credible. The vehicles through which this is happening are still maturing, but the direction of travel is clear. Investment funds, financing platforms, and blended capital structures are no longer experimental. They are all becoming the institutional architecture of a new economic statecraft.

Countries that coordinate their financing efforts with trusted partners across the private and public sectors will secure the industrial capacity and long-term advantages that come from the multiplier effect of acting together to pool capital. This is even more important in competition with adversaries who can direct state-backed financial resources.

Mobilizing the Full Allied Capital Stack

Funding critical industries requires the full capital stack working together across the entire supply chain. Public and private capital have already begun organizing around technology opportunities, but the infrastructure, manufacturing, and energy systems that underpin these industries demand much larger and more varied sources of finance. Different segments of the capital stack, from venture capital to development finance institutions to sovereign wealth funds and pension systems, play distinct roles.

Capital-rich markets such as the Middle East illustrate how large pools of capital translate directly into economic influence. Investment institutions such as Mubadala, the Abu Dhabi Investment Authority, Saudi Arabia's Public Investment Fund, and the Qatar Investment Authority play a leading role in funding critical industries around the globe.[106]

However, where capital originates matters because the financial returns, governance influence, and long-term industrial relationships that follow tend to flow back to the capital provider. For the United States and its allies, relying heavily on external financing for strategic industries risks shifting both economic benefit and strategic influence to potentially unfriendly actors.

Crucially, many of the largest pools of capital sit within allied economies. Pension funds and sovereign wealth funds are well-suited to financing long-term infrastructure, though fiduciary caution is an important consideration. Australia's pension system manages more than $2.5 trillion.[107] Japan's Government Pension Investment Fund and related institutional investors represent even larger pools of capital, which play a stabilizing and leadership role due to their long term (often 100 year) investment return horizon and experience in infrastructure investment, in the region.[108]

At the same time, private finance is increasingly identifying commercial opportunities across critical industries. JP Morgan's 2025 commitment of $1.5 trillion over 10 years across advanced manufacturing, defense, aerospace, energy, and frontier technologies reflects a broader market trend toward economic security as an investment category.[109]

The question now is not whether capital exists to fund critical industries, but whether governments and allies can organize the full capital stack quickly enough to direct it toward shared strategic priorities.

Rewiring Economic Statecraft: A Policy Agenda

Meeting this challenge requires governments and industry to focus on several areas where policy and capital markets intersect.

LOWERING THE COST OF CAPITAL

For starters, governments should focus on reducing the cost of capital to encourage large-scale private sector capital into critical industries. Many critical industry projects require advanced manufacturing, energy infrastructure, and digital systems, which involve long horizons and significant upfront investment. New legislation in the United States provides one example of how governments can influence capital flows. By allowing businesses to immediately deduct the full cost of eligible machinery, equipment, and certain property improvements in the first year on their taxable income, rather than spreading the expense over several years, the policy reduces the cost of capital and accelerates private sector investment.[110]

ENABLING PRIORITY PROJECTS

Many governments already maintain national priority infrastructure to signal investment focus. Australia's Infrastructure Priority List, the United Kingdom's Planning and Infrastructure Bill, and Indonesia's National Strategic Projects scheme all serve precisely this function.[111]

A logical extension for these national models would be the creation of a shared priority list across allies and partners. A multilateral critical industries list would signal clearly where large-scale capital deployment is required. Establishing such a list would require credible coordination across governments and some form of repository or coordinating body.

Strategic competition in this area is already well-embedded, with China's Belt and Road Initiative and institutions such as the Asia Infrastructure Investment Bank combining project identification and financing at scale. Yet the Belt and Road Initiative's record is instructive in a different sense, as country trust has eroded over time.[112] The allied model's comparative advantage is precisely its credibility: transparent standards, genuine co-investment, and governance structures that give partner countries agency rather than dependency. That is not a constraint on allied economic statecraft — it is its most durable competitive asset.

Allied coordination in this area is nascent but accelerating. The Trilateral Infrastructure Partnership, launched in 2018 by the United States, Japan, and Australia, offers a cautionary precedent.[113] Despite best efforts, it struggled to align investment mandates, pool capital, generate shared demand signals, or establish a clear project pipeline, functioning ultimately as a coordination framework rather than a decisive financing mechanism. Evolved models include the Indo-Pacific Partnership for Prosperity, which brought together $25 billion worth of capital to invest in the region, and the very recent Indo-Pacific Energy Security Ministerial and Business Forum, which aims to support coordination and project deal-making.[114]

However, U.S. allies and partners have not yet developed mechanisms to align their infrastructure priorities, finance tools, and private sector across an allied network that can withstand political changes. The generative AI-led boom may be the forcing function that changes this. The scale of its demand is so fundamental, and the consequences of falling behind so significant, that it creates a rare opportunity to build coordination mechanisms that transcend political cycles and are private sector-led.

AGGREGATING DEMAND ACROSS ALLIES

Governments and industry have a role to play in ensuring that demand for critical industry assets reaches the scale necessary to justify major investments. From subsea electrical and digital cables, support operations like construction and repair vessels, to grid equipment, to manufacturing facilities, and advanced energy systems. These all require long-term production volumes to attract manufacturing facilities and infrastructure financing.

Allies are beginning to experiment with mechanisms that combine project finance, supply chain coordination, and early forms of pooled demand. The critical minerals sector provides an emerging reference point. Initiatives such as the Forum on Resource Geostrategic Engagement, the Quad Critical Minerals Initiative, and the U.S.-Australia Framework for Securing Supply of Critical Minerals and Rare Earths reflect growing recognition that securing critical mineral inputs for advanced manufacturing, energy systems, and defense capabilities requires multilateral coordination.[115] Financing cooperation is also emerging. The recently announced U.S. Critical Minerals Strategic Reserve would allow companies to pre-sell future output to governments or industrial buyers, quarantining them from shocks in the future to demand.[116]

In other areas, there are examples of regional energy power pools, food and health demand pooling, or the pooling of fuel reserves by the International Energy Agency, which are areas to examine (although the organization's efforts in effect coordinate the release of fuel rather than physical aggregation).[117]

Taken together, these steps represent various forms and levels of allied industrial cooperation by aggregating demand for certain key components. In the future, demands should be extended to the full spectrum of physical assets, including industrial manufacturing capacity and purchasing and demand aggregation.

BUILDING FINANCING PLATFORMS

Governments should adapt lessons from technology-focused finance vehicles like the NATO Innovation Fund to critical industries. Given the significance of the Indo-Pacific for the United States and in the quickly evolving generative AI boom, countries could look to establish a dedicated Indo-Pacific critical industries fund that could align capital and strategic priorities across a range of different investment opportunities within the sector. Such a vehicle could be financed by the public and private sectors for large-scale investments that are appropriate for significant capital expenditure projects or supply chains. They could also include a backbone support organization to inform building the enabling environment, information sharing, and convening between governments and the private sector.[118] Given their prior lessons and learnings in investment in the region, Japan and Australia are natural anchor partners for such a vehicle with the United States, given their financial resources, including large pension fund capability, and historical and current experience in investing in the Indo-Pacific. If a regional critical industries fund were to be established, it could also be linked to a shared critical infrastructure list between allies and partners. This would be especially helpful when

governments need to convey their dual-use infrastructure requirements across the Indo-Pacific to private sector lenders and investors.[119]

IMPROVING GOVERNMENT COORDINATION

Each government should consider a special envoy office with clear authority to coordinate critical industries policy across government and industry. That office will need authority and ability to reach into key departments such as defense, energy, finance, trade, and industry, and have the cut-through with industry, particularly the finance community. This office should function as a coordination mechanism across government agencies, between countries, and between governments and industry.

ACCOUNTING FOR STRATEGIC ECONOMIC VALUE

Finally, governments should confront a broader analytical challenge. Current fiscal frameworks struggle to capture the wider strategic value created by infrastructure investments, which are often evaluated only through traditional metrics such as jobs and growth. Developing shared metrics across allied economies would help governments justify long-term investments in critical industries.

Mastering the financial, physical infrastructure, and technological layers of economic statecraft — and coordination across them — is no longer optional. It is the defining challenge of strategic competition in the AI-infrastructure boom era.

The pace and shape of this coordination will inevitably be shaped by the disposition of the United States at any given moment. When Washington is an active lead partner, allies can move further and faster. Alternatively, when U.S. posture is more transactional, the case for allies building a more resilient, self-reinforcing financing architecture of their own becomes correspondingly stronger.

Emerging contemporary economic statecraft is about the sustained organization of capital across critical industries, building resilience, deterrence, and long-term industrial capacity that national and global security now demands. The countries that grasp this and act on it together will define the strategic landscape and capture the value of the AI infrastructure-led boom for generations to come.

Georgie Skipper is a Fulbright scholar and former senior advisor to the Australian foreign minister. She is the CEO of Lucetia Group, a co-founder and affiliate director at the Massachusetts Institute of Technology Murray Lab for Geopolitics and Innovation, and a research affiliate at the Massachusetts Institute of Technology Sloan School of Management.

The implication is clear: the countries that organize capital, energy supply, and infrastructure fastest will shape where the AI economy ultimately scales and who gains from the value creation.

CHAPTER 4 EPILOGUE: WHERE THE FRONT LINE MEETS THE BALANCE SHEET – COMBATANT COMMANDS AND CONTEMPORARY ECONOMIC STATECRAFT

Georgie Skipper

Geographic combatant commanders sit at the seam of diplomacy, security, and economics in their theaters. The thesis explored in the previous article, that the ability to mobilize and direct large pools of public and private capital across critical industries is becoming the defining instrument of contemporary economic statecraft, is now playing out in real time for American combatant commands.

The terrain that enables stability, security, regional cooperation, and peaceful development is being shaped by diffuse actors and pressures. Energy security, the digital and AI build-out, vast equipment requirements, dual-use innovation, manufacturing, and recovery from natural disasters all demand financing at scale, and more of that responsibility is landing in commercial hands. Partner governments navigate their own exposure to China, Russia, and other actors as they consider who builds and manufactures, whose technology is procured, and who finances critical infrastructure developments in their own economies. The principles explored here apply across all the geographic regions. This article concentrates on the Indo-Pacific, where critical and strategic infrastructure sits at the center of an evolving landscape in which the levers of contemporary economic statecraft are tested daily.

American operations in the region depend on assets the U.S. alone does not necessarily own and rarely finances. The regional build-out now underway, and the gap in how it is financed, will determine who holds leverage over assets and, therefore, capability. Financing instruments have therefore become security instruments, and the U.S. needs the institutional machinery to treat them that way. The state's leverage now flows from what it commits to buy. The government is becoming a customer, and its custom is an instrument of statecraft.

The Stakes for the United States

The stakes are concrete. They begin with the bases the United States operates and the sites it needs access to. They extend through the infrastructure that supports operations, from cyber-secure networks to reliable energy. Presence in peacetime requires stable use of those assets. Conflict requires entering, operating from, and flying through the region. Both rest on ports, airfields, grids, and cables working on the day, and every day after.

Looking at the theater in a more integrated way, American requirements extend in two directions. The first concerns American strategic needs. Take critical minerals, of which an abundance is in the Indo-Pacific: securing them creates a requirement for ports, processing, and transport infrastructure in partner countries. The second concerns the partners themselves, and the net benefits of stronger partner countries. The United States needs regional partners that prosper from the build-out, gaining technology, jobs, and economic benefit from what is built on their soil. Partners that benefit make an Indo-Pacific that is stable and fit for peaceful development, and willing to host the presence that keeps it so. That same build-out should leave partners less exposed to Chinese capital and technology or ensure that China cannot convert its existing investment into leverage.

The pattern repeats across critical industries, whether the issue is energy, digital infrastructure, facilitating assets like ports and roads, strategic infrastructure that meets military requirements, critical minerals, or manufacturing. All of it is under strain. American power is protected and projected through assets the U.S. may neither own nor finance. Increasingly, the United States relies

on assets and actors beyond its direct control to achieve its goals in the region. The question that follows is who does own and finance those assets, and on what terms.

The Regional Financing Gap

The scale of the need across critical industries is great. The International Energy Agency estimates that more than $300 billion is required to expand and modernize Southeast Asia's electricity grids between 2025 and 2040.[120] Annual data center investment across the Asia-Pacific reached roughly $102 billion in 2024 and is projected to approach $175 billion by 2030.[121] Some of this infrastructure requires modernization; some must be newly built. Conventional financing is limited in what it can deliver at scale. Poor sovereign credit ratings, permitting and right-of-way barriers, difficulty repatriating returns, and thin technical capacity have strained how critical infrastructure gets financed. Vulnerable partner infrastructure is exposed to cyber and other forms of disruption. Since the Belt and Road Initiative, China has matured into a leading funder of the assets in question. In the Philippines, the national transmission network operates under a concession in which China's state grid company holds a 40 percent stake.[122] Whoever fills the financing gap acquires the leverage, and the leverage lands on the same assets American operations depend on.

Financing as a Security Instrument and Coordination Mechanism

Where creative financing has been applied, the results are instructive, and they are pathfinders for a new economic statecraft landscape in areas of responsibility. Subsea telecommunication cables show the pattern most clearly. Washington is now moving to institutionalize that role through the bipartisan Strategic Subsea Cables Act of 2026, which would create a dedicated interagency committee, expand State Department capacity on cable security, and mandate sanctions for those who intentionally damage undersea infrastructure. American technology companies are part of the same effort: new trans-Pacific cable systems backed by Google and Meta have been routed through Indonesian and Philippine waters specifically to avoid the South China Sea.[123] The pattern extends beyond cables. Sri Lanka, rich in graphite and short of currency reserves, is seeking American investment that would carry port access with it.[124] Creating, hardening and holding assets of this kind is a precondition for wartime access and peacetime confidence alike, and it takes support and coordination from private finance.

Commercial and security requirements are increasingly entwined in the same assets. The grid that powers a partner economy powers the airfield a command would surge through. The cable that carries commerce carries command and control. The port that serves container traffic serves military sustainment. Ownership and financing of those assets affect strategy and execution. The instruments that work have hallmarks familiar from established infrastructure finance: pre-committed government revenue streams, conditional offtake agreements, blended public-private structures, economic opportunity zones, and plug-and-play maintenance and repair zones.

Traditional infrastructure public-private partnerships begin with the customer identifying its requirements and stating its offtake clearly, and the same discipline applies to strategic assets: when a government can state how many days or months a port or shipyard will be needed each year, commercial structuring becomes possible around that commitment. Subic Bay is an instructive case in point. When a private investor moved to acquire the former shipyard, the United States government pre-committed revenue contracts, with the award conditional on the acquisition completing. That commitment guaranteed utilization and revenue from the first day of ownership, de-risked the asset before purchase, and allowed the investor to clear its own internal approvals.[125] The approach has precedent: the United Kingdom, Australia, and the Netherlands have each used public-private partnerships, private construction financing, or sale-and-leaseback structures to upgrade defense facilities while freeing public capital for other uses.[126]

The emergence of dual-use infrastructure is a key part of the economic statecraft toolkit. This is

because an asset serving commercial and security users at once has a broader revenue base, which makes it more investable and more affordable than a dedicated facility either side would build alone.[127]

Structuring solves the investor's side of the problem. Financing becomes a strategic instrument. Agreements that recognize the economic benefits flowing to host nations convert infrastructure from an imposition into a shared asset, which is what makes the politics of hosting it sustainable.

The same logic now runs through dual-use technologies. A new class of manufacturer, funded by private capital across hard and soft capability, is helping to meet a new demand fueled by conflict. Venture capital now performs the function the government's research and development budget once performed: investors fund the development risk, the company arrives with a working product, and the government becomes a customer. That is why new entrants move at higher speed and lower cost. The state is the anchor customer.

Institutionalizing Economic Statecraft

The mission of the United States in the Pacific is to enhance stability by promoting security cooperation, encouraging peaceful development, responding to contingencies, deterring aggression and, when necessary, prevailing in conflict. That mission can no longer be performed well without drawing on economic statecraft, because the terrain it is performed on is financed, built, owned, and operated by an array of different stakeholders. An institutionalized response would require: an economic statecraft capability inside the command that fuses intelligence on capital flows with operational planning; a standing interface with the investors active in the critical industries in the areas of responsibility; and input into allied financing decisions, wherever a guarantee or an offtake would do as much for access and resilience as for exercise.

Finance has become central to how allies and partners coordinate on critical industries. Ukraine reaching into Russian energy infrastructure and the recurring contest over the Strait of Hormuz show what happens when economics and operations converge in a theater. In the Indo-Pacific, they are converging in advance of conflict. That is the window in which institutions can still be built, and a command that can shape where capital flows in its theater, which, if done well, is practicing integrated deterrence in its most concrete form.

Georgie Skipper is a Fulbright scholar and former senior advisor to the Australian foreign minister. She is the CEO of Lucetia Group, a co-founder and affiliate director at the Massachusetts Institute of Technology Murray Lab for Geopolitics and Innovation, and a research affiliate at the Massachusetts Institute of Technology Sloan School of Management.



CHAPTER 5

ABSTRACT

The defense budget is the federal government's largest instrument of economic statecraft, whether or not the Pentagon treats it that way. Defense accounts for roughly half of U.S. government discretionary spending, yet private capital dwarfs it, and at that scale steering even modest changes in private investment can have effects similar to or greater than those of new government appropriations. The article frames the obstacle to coherent private-public orchestration of economic statecraft as a signal-to-noise problem: defense budget guidance names priorities far beyond what the budget can fund, and the demand signals industry needs arrive scattered and inconsistent.

To strengthen the signal, the department should weave economic statecraft assumptions into the Defense Planning Guidance and have each service publish structured demand signals tied to those priorities. To steady the budget for industry, the article proposes common data standards tagging programs to missions and industrial dependencies, a return to the pre-2010 two-year internal budget cycle, and growth in the funds that carry technologies from lab to program of record.

Scan the QR code to view the webinar that accompanies Chapter 5.

SHARPENING SIGNALS AND REDUCING NOISE FOR BETTER DEFENSE BUDGETS

Mark Mitchum

Debates over defense budgets and economic statecraft are not a distraction from warfighting. They reflect a basic reality: Military power does not exist in isolation. It is built, sustained, and ultimately limited by America's economic capacity and the system that translates resources into capability.

The United States cannot compete with high-end adversaries if it cannot convert economic strength into fielded capability. That linkage — between resources, industry, and operational output — is what determines whether national power materializes in armed conflict.

America's advantage lies in free markets and competition, not centralization. The military will outperform rivals by leveraging the dynamism of its own economy. That advantage depends on sending clear signals to both the force and industry about priorities and demand.

Improving outcomes is less about top-line increases or sweeping reform than about coherence. The Department of Defense's budget process should communicate stable intent. Better guidance, more consistent engagement with industry, and stronger data inputs can help to reduce noise and sharpen those signals.

Inextricably Connected

Why is a discussion of defense budgets part of a series on economic statecraft? While building better budgets does not inherently equate to better economic statecraft and vice versa, three factors increasingly link these efforts.

First, the sheer scale of defense spending relative to overall discretionary federal spending is substantial. For Fiscal Year 2024, the Congressional Budget Office reports that defense accounted for approximately 47 percent of discretionary spending.[128] Defense supplementals and reconciliation authorizations will likely shift this proportion upward in future years. In other words, the Defense Department accounts for roughly half of the federal government's available funding. Regarding the "promote authority" discussed in another article in this series, the defense budget is the largest single mechanism within the federal government to drive action.[129] There is no way to effectively wield the incentives of federal spending without viewing the defense budget as a way to both achieve hard power results and drive national economic statecraft outcomes.

Second, the Pentagon is deeply dependent on industry and the broader economy to produce and sustain capability advantages over competitors and adversaries. While the military instrument of U.S. hard power is visible and tangible, the innovative and entrepreneurial capacity of the United States forms the foundation of national competitive advantage. If national security priorities are not translated into clear defense budgetary signals, industry and private capital will not align to solve key national security challenges, and America will fail to harness its innovative industrial ecosystem.

Finally, the process and behavioral changes required to use the defense budget as a tool of economic statecraft are nearly identical to the changes required to produce better military outcomes.

Demystifying the Defense Budget Process

Understanding the connection between the defense budget and economic statecraft requires a brief explanation of the seemingly impenetrable Department of Defense budgeting system, known as Planning, Programming, Budgeting, and Execution.[130] This is essentially a collection of interdependent processes that translate the president's strategic guidance into the department's annual budget submission. (To simplify, I use "budget process" to describe the overall process. Technically "budgeting" is a narrow comptroller function).

The budget process seeks to align resources to achieve objectives outlined in strategic guidance, such as the *National Security Strategy* and the *National Defense Strategy*. Derived from those documents, the *Defense Planning Guidance* underpins the budget process and translates policy objectives into specific priorities for each portion of the immense defense enterprise. This annual guidance sets the conditions and assumptions used to build and assess budget inputs. Unfortunately, the guidance tends to identify priorities far beyond realistic funding levels. Typically, this means that for every $10 billion of "priority" capabilities, there is less — usually far less — than $1 billion available to pay for them. This deficit effectively neuters the guidance and produces a nearly incomprehensible compilation of parochial budget priorities.

For example, consider the dilemma the Air Force faces as it simultaneously attempts to maintain current operations, increase readiness for future conflicts, and modernize its aging fleet. Like all the services, the Air Force's budget essentially breaks down into three bins: manpower (paying military members and civilian employees), readiness (fuel, maintenance, training), and modernization (developing and buying systems). Consequently, a seemingly massive, approximately $200 billion annual budget rapidly closes in on itself. Historically, about one-third of the budget is aligned to modernization, encompassing research, development, test, evaluation, and procurement. Nuclear modernization and multi-year programs add further budgetary constraints.[131] Combined with the fiscal disconnect of the *Defense Planning Guidance*, this results in an annual exercise of balancing near-term readiness and long-term modernization risk. Similar tradeoffs play out across each service and agency in the defense enterprise.

Consider shipbuilding, secure semiconductor sourcing, and space launch — all examples of defense-centric decisions with implications far beyond the Pentagon's purview. The military services and defense agencies receive little to no direction on incorporating broader economic statecraft considerations into their budget calculus. Therefore, services spend years constructing budgets based on force structure, requirements, and policy assumptions that potentially fail to address broader national goals. Late-stage inclusion of new factors in the budget process — such as expanding the defense industrial base — invariably leads to fiscal disconnects between the services, across programs, and appropriations requests. This dynamic undermines the coherence of defense budgets and points to the need for improved initial guidance.

Commercial Markets and Defense Budgets — Scale and Opportunity

While defense spending accounts for an outsized portion of federal spending, it is still dwarfed by the investments across commercial industry — this presents challenges and opportunities. The current acceleration and democratization of manufacturing and innovation are paired with a reemergence of dual-use technologies that allow advanced militaries to leverage private capital. For example, Goldman Sachs estimates that AI companies may invest more than $500 billion in 2026.[132] By comparison, the Trump administration's 2025 budget request submitted to Congress was $310.7 billion in all defense investment accounts combined.[133] While reconciliation and other congressional actions ultimately increased this figure, it remains far below private sector investments in a single sector.

In this environment, influencing small changes in the trajectory of private sector investments represents a *de facto* increase in defense spending. Importantly, this logic not only applies to the United

States, but its allies, partners, and adversaries as well. The fundamental question going forward is how the U.S. defense establishment should navigate and optimize these opportunities to create relative capability gains.

The following examples highlight the linkages between defense budgets and economic statecraft.

Dual-Use Heavy Manufacturing Considerations — Aerial Refueling

Consider a case in which an individual military program has far-reaching national economic competitiveness implications. The Air Force provides global aerial refueling capacity with a fleet of approximately 465 tanker aircraft. Over three-quarters of that fleet is made up of the aging KC-135 aircraft, a Boeing 707 derivative, which first entered service in 1957. A steady state of global operations are straining the fleet, including nuclear deterrence, training, and homeland defense. In major conflict, aerial refueling is a force projection enabler but also an operational dependency. Recent events and reporting highlight the inherent risk of air refueling and forward basing, but also the difficulty of rapidly replacing this aging fleet.[134]

The Air Force is slowly replacing its KC-135s on a one-for-one basis with the Boeing KC-46 Pegasus, a military derivative of the 767 airliner. The service received its 100th aircraft in Dec. 2025 and Boeing plans to deliver an additional 19 KC-46s in 2026.[135] The KC-46 shares a production line with the 767 freighter, the last commercial variant of the airliner, which is not commercially viable without sustained tanker production. Therefore, the fate of a domestic dual-use heavy aircraft production line, a fleetingly rare national asset, is inextricably tied to year-to-year Department of Defense budget decisions which take little account of broader national economic impacts.

The KC-46 is just one example of the connection between domestic aircraft production and military capabilities. Global competitors in the commercial aircraft market put pressure on Boeing, one of the largest historical exporters and military suppliers in the United States.[136] Meanwhile, the development of new dual-use domestic aircraft manufacturing capabilities, such as blended wing body designs, require coordinated policy action to incentivize investment, build manufacturing capacity, and accelerate certification.[137] These issues span the Departments of Commerce, Transportation, and Defense, among others, but there is no clear coordination function for unified action. The largest federal fiscal signal remains the defense budget with no clear mechanism for consideration of these broader issues.

Production as Military Capability — Munitions

Nowhere is the mismatch between defense budget decision-making and battlefield reality more evident than in modern munitions. A recent *Washington Post* article highlighted the disparity between expenditure and production rates of weapons such as the Tomahawk Land Attack Missile and Patriot interceptor missiles.[138] These two high-end systems represent a larger class of expensive weapons that are highly capable but rely on complex, bespoke, and overlapping supply chains. This is the result of many factors, including industry consolidation, accumulated annual budget decisions that drive down production rates, and requirements processes that privilege "exquisite" over "good enough" solutions. Regardless of cause, the result is using $3 million munitions to destroy $35,000 Iranian Shahed drones, with limited room for rapidly increasing production. This is simply unsustainable.[139]

The rapid growth of the additive and distributed manufacturing ecosystem offers opportunities across the munitions portfolio. Not only can this new ecosystem accelerate fielding of systems at scale with reduced costs, but it also provides a manufacturing infrastructure capable of rapid adaptation. An influx of venture capital investment in defense technology is helping build a robust manufacturing ecosystem, but investors must continue to see a clear path to returns.[140] The lack of a coherent and consistent demand signal from the Department of Defense risks undermining the perceived value of these investments and squandering a critical opportunity.

The air refueling and munitions examples highlight the need for coordinated action between

government and the private sector. Ultimately, economic statecraft tools like federal and state tax incentives, intellectual property protections and public-private cost-sharing agreements are inseparable from defense policy and budget discussions.

It's a Signal-to-Noise Problem

William Norris' article in this series addressed ways to improve national policy and interagency coordination mechanisms, but there are practical, near-term improvements the Department of Defense should implement now.[141]

Improving ties between the defense budget and broader economic statecraft priorities requires improving the signal-to-noise ratio: increasing the signal internally with improved guidance and externally through better communication with industry, while reducing noise by removing unnecessary processes, increasing stability for investors and suppliers, and sharing a common view of capability and industrial impacts of decisions.

The following recommendations are designed to improve defense budget coherence and better integrate economic statecraft into Defense Department decision-making.

Strengthen the Signal

INCORPORATE ECONOMIC STATECRAFT GUIDANCE IN THE *DEFENSE PLANNING GUIDANCE*

The department should incorporate economic statecraft considerations and assumptions in guidance provided to the military services through the *Defense Planning Guidance*. First, the guidance should consider fiscal constraints in its stated priorities for investment and risk acceptance and more robustly address costs beyond the current five-year window. Second, the guidance should provide clear priorities and assumptions related to industrial policy. Third, this guidance should include measurable and assessable criteria with specific emphasis on addressing the cost imbalance highlighted by the Shahed example. Ultimately, shifting funds is the most powerful bureaucratic incentive — organizations will respond to this guidance if it drives budget decisions.

PUBLISH DEFENSE-WIDE AND SERVICE DEMAND SIGNALS TO INDUSTRY

Private capital now plays a decisive role in defense innovation, yet the Department's demand signal remains fragmented and episodic. The Department should mandate that each service publish structured, problem-centric industry demand signals tied to *Defense Planning Guidance* priorities. This is not a substitute for requirements documentation, but it affords industry insight into resourcing intentions. Clear signals allow investors to allocate capital earlier, enable industry to build bridge markets across commercial and defense sectors, and help new entrants align designs with realistic production and sustainment assumptions. This recommendation is likely the easiest and most consequential action the Department of Defense can take to align economic statecraft efforts and the defense budget process.

Reduce the Noise

MANDATE COMMON LEXICON AND DATA FIELD USE ACROSS THE DEFENSE BUDGET PROCESS

To integrate economic statecraft considerations into defense planning, the Department of Defense should see itself clearly. Today, requirements, force design, acquisition, budgeting, sustainment, and industrial base assessments operate on overlapping but inconsistent taxonomies and data structures. Capability-focused methodologies help decision-makers understand the operational context and dependencies inherent in budget decisions. The Department should build on efforts like "mission engineering" analysis, which maps the programs and systems required to accomplish a mission. The Department should mandate "tagging" programs to missions, industrial dependencies, surge capacity, supply chain exposure, projected operating-to-acquisition cost ratios, and relevance to national economic priorities. This does not require a new billion-dollar system of record — simply publish and enforce data standards. Once visible, tradeoffs become clearer, and the complexity becomes governable.

RETURN TO TWO-YEAR INTERNAL BUDGET CYCLES

The current annual budget process within the Defense Department paradoxically leads to less budget flexibility, insufficient analysis, and less stability for external stakeholders. Prior to the 2010 budget, the department provided an annual budget input Congress but internally performed a two-year cycle.[142] This approach provides increased time for analysis and decision-making, leading to better decisions, especially those impacting major modernization programs. While business rules can still allow annual changes to maximize opportunities, the increased analysis will improve stability for industry, supply chains, and Congress.

BUILD PROGRAMMATIC STABILITY WHILE ADDING FLEXIBILITY

Leveraging private capital in defense technologies often requires relatively small, flexible increments of funding — tens of millions of dollars versus billions. The critical funding gap often is the one-to-three-year bridge between lab investments and longer-term program of record funding. Current technology transition accounts allow the services to become critical late-stage investors and spur additional private funding. To avoid the typical three-year service budget lag these funds are appropriated with spend plan level detail and updated as opportunities emerge. Modest funding increases to these accounts complement a two-year budget cycle by improving stability within established programs while also increasing flexibility for emerging capabilities.

To outpace its adversaries, the United States should harness its competitive strengths to generate economic power and translate it into enduring military advantage. Improving the signal-to-noise ratio in defense budgets offers a practical, near-term path to aligning innovation, industry, and investment with the demands of modern conflict.

Mark Mitchum is a retired U.S. Air Force major general and former commander of the Air Force's provisional Integrated Capabilities Command, with deep experience in planning, programming, and requirements. He founded StratAero Advisory, where he advises clients on strategy, investment, and capital allocation.

There is no way to effectively wield the incentives of federal spending without viewing the defense budget as a way to both achieve hard power results and drive national economic statecraft outcomes.

CHAPTER 5 EPILOGUE: TOO MUCH COWBELL? WHEN DEMAND SIGNALS BECOME NOISE

Mark Mitchum

In a famous Saturday Night Live sketch, Christopher Walken insists Will Ferrell keep adding "more cowbell" during a recording session. To our eternal enjoyment, the underlying track is lost in the overpowering, atonal din. Too much of a good thing is, in fact, too much.

The Pentagon risks replicating this mistake. America's industrial capacity and capital markets are a significant competitive advantage, but only if properly incentivized. My earlier contribution to this series argued that the budget process often impedes the industrial base by providing insufficient demand signals.[143] That argument still holds, but it carries a corollary: increased signal without prioritization becomes noise.

Fiscally unrealistic demand signals lack credibility, misdirect capital, and inflict long-term harm on the defense enterprise.

THE ROLE OF DEMAND SIGNALS

In the complex and sprawling defense enterprise, demand signals play a critical role in synchronizing disparate activities to advance national security. Demand signals are far more than signed contracts. Done correctly, the signals see beyond the immediate budget environment and provide program offices, industry, Congress, and academia with a common understanding of the environment, challenges, and priorities for future resourcing. This implies a decreasing level of specificity as time horizons expand. It also requires a level of fiscal reality that helps diverse actors in the economy align capital against the most important gaps and those most likely to receive funding.

THE MULTIYEAR PARADOX

The most concrete demand signal is a signed and funded contract. But even major programs of record carry surprising uncertainty, as evidenced by sharp year-to-year changes in procurement quantities across systems as diverse as $100 million F-35s and $300,000 Javelin missiles.[144] These changes impact every layer of the supply chain and drive inefficiencies and hedging. Multiyear contracts are an effective mechanism to reduce these annual changes and provide stability to the industrial base. These multiyear agreements span the near- and mid-term gap and are strong motivators to incentivize infrastructure investment and capital expenditures.

The ability to write multiyear contracts was a hard-earned advance between the Pentagon and Congress. In the fiscal year 2023 defense authorization, Congress extended multiyear authority to a long list of critical munitions.[145] When used correctly, this approach provides stability to suppliers by removing the constant year-over-year budget-driven variations in procurement rates. But authorization is not appropriation. The budget is still approved in annual increments and future funding commitments inherently carry risks in the face of uncertain budgets. This is among the reasons the Pentagon and Congress were slow to actually utilize these authorities at scale.

The paradox runs even deeper. Multiyear procurements earn savings when quantities are held stable and fully funded across the contract period. An aspirational commitment trimmed in the out-years erodes the very economies of scale that justified the authority in the first place. The tool meant to reward and incentivize commitment ends up penalizing it.

DEMAND WITHOUT BUDGET

The drawdown of high-end munitions in the recent conflict with Iran is substantial, and the need to replenish stockpiles is pressing.[146] This urgency encourages the Department to signal maximum demand across too many programs simultaneously.

Recently the Department of Defense moved to dramatically expand the use of multiyear agreements and contracts. In August 2025, the Pentagon awarded $7.8 billion in multi-lot production contracts for additional missiles.[147] In July 2026, a seven-year Patriot interceptor agreement worth up to $58.6 billion was announced, replacing a single-year award made just three months earlier.[148] An additional wave of multiyear framework agreements now covers Tomahawk, the Standard Missile family, the Precision Strike Missile, and a new class of low-cost cruise missiles, most promising production rates two to four times current output.[149] But several of those agreements only convert to multiyear contracts with new congressional authorization and subsequent appropriations.

Meanwhile, the Pentagon is publicizing its plan to mass-produce low-cost hypersonic and long-range strike weapons in massive quantities over the next five to six years.[150] Taken individually, the multiyear commitments and affordable mass announcements make sense, but collectively the stated demand exceeds even the most bullish budget assumptions. In the near term, a meaningful share of the current missile procurement request depends on highly uncertain reconciliation funding.[151] In the longer term, a significant portion of the anticipated demand only materializes if future defense budgets achieve and maintain ahistorical growth rates. Ultimately, the new multiyear munitions demand signal lacks prioritization, fails to account for realistic budgets, and provides false precision in the medium term.

CONCENTRATING RISK

A demand spike that collapses in two years will fail to produce a meaningful increase in munitions production and risks sowing the seeds of lasting damage. This scenario, which is very possible, teaches industry, and the capital markets, to discount future demand signals and seek higher risk-adjusted rates of return.

For large prime contractors, responding to a multiyear signal means committing capital to new lines, tooling, facilities, and hiring. The financial performance of these publicly traded companies is assessed using metrics such as return on invested capital. When infrastructure investments fail to produce revenue, the stranded capital depresses returns and markets respond accordingly. Corporate boards and investors will respond by applying a higher risk premium to future defense demand.

The more consequential risk sits a tier or two down, where suppliers tool up and hire to meet expected demand. These are the makers of specialty chemicals, castings, forgings, and numerous subcomponents. Many of those specialized markets have only a handful of suppliers, and in some cases they are essentially sole source.[152] While undesirable, most primes can absorb a limited number of stranded investments on a large balance sheet. A specialty supplier often cannot bridge these stranded investments and risks bankruptcy. Such failures do not simply reduce capacity. In some cases the capacity and the workforce disappear. Through this lens, aspirational signaling concentrates risk precisely where the industrial base is least resilient.

Compared to the primes, nontraditional defense entrants face a different capital problem. Their survival often depends on continued private investment. When demand projections repeatedly fail to materialize, investors will not simply discount the deal. They begin to fundamentally question whether the defense technology investment thesis is valid. That doubt risks capital flight and undermines America's capital markets advantage. This is a real threat to the Pentagon's increasing reliance on these firms to affordably manufacture at scale.

CREDIBLE AMBITION

Ambition is not the enemy, but credibility is the currency that produces real capacity. Individual demand signals do not exist in isolation. Each is part of a larger whole, and they aggregate at three levels that must each hold up on their own. Within a portfolio, such as munitions, the collection of programs and signals must tell a coherent story over multiple time horizons. Within a service, the portfolios must reasonably fit within a top-line budget that accounts for total costs to organize, train, and equip the force. At the Department of Defense level, the services' aggregate demands must collectively further the national security strategy and fall within

a realistic budget trajectory. A signal can appear credible at one level and incoherent at the next. A healthy defense industrial base requires coherence across all three levels.

Aligning America's economic capacity toward fixing its hardest defense problems requires better, not perfect, demand signals. A specific and funded near-term signal, paired with an honest and directional long-term signal, will reduce hedging and unleash productive market forces. It also maintains the Pentagon's standing with industry, the markets, Congress, and, most importantly, our adversaries. Clarity was the argument of my first article. Credibility is its necessary companion. A little cowbell carries the song. Too much cowbell buries the music.

Mark Mitchum is a retired U.S. Air Force major general and former commander of the Air Force's provisional Integrated Capabilities Command, with deep experience in planning, programming, and requirements. He founded StratAero Advisory, where he advises clients on strategy, investment, and capital allocation.

Ambition is not the enemy, but credibility is the currency that produces real capacity.





CHAPTER 6

ABSTRACT

Economic statecraft has become a decisive component of modern warfare, with supply chains increasingly shaping military outcomes before combat begins. Although the Pentagon has launched initiatives to strengthen economic resilience (like the Office of Strategic Capital, and the Economic Defense Unit), it lacks an integrating capability at the very top of the Department to strategically assess and mitigate supply chain vulnerabilities, coordinate interagency investments, and build stronger partnerships with industry that impact military missions.

Dr. Kellogg advocates establishing an entity like the previously proposed Economic Warfare Operations Capability within the Pentagon to provide commanders with tools for evaluating economic risk, improving supply chain visibility, fostering private-sector cooperation, and incorporating economic statecraft into military education and operational planning. By institutionalizing these functions, the United States would be better positioned to compete in an era where economic leverage is as strategically significant as conventional military power.

Scan the QR code to view the webinar that accompanies Chapter 6.

OPERATIONALIZING ECONOMIC STATECRAFT: A NEW IMPERATIVE FOR THE PENTAGON

Anita R. Kellogg

The next major war the United States fights could be decided by supply chains long before the first shot is fired. That reality is already taking shape, as adversaries use export controls, sanctions, and supply chain leverage to shape outcomes on the battlefield.

The Russo-Ukrainian War typifies this development: China has enacted strict export restrictions on drones and drone parts bound for Ukraine, directly degrading its military capability.[153] In response, Ukraine has developed a China-free drone, though cost pressures continue to drive reliance on Chinese components.[154]

This is not an isolated case. Sanctions that specifically target military technology have grown more prominent in recent years. The United States and its allies have imposed export controls on China for advanced semiconductor chips and the tools made to produce them. China, in turn, has restricted rare earth sales to firms working with the Pentagon — putting nearly a third of defense procurement programs at risk of shortages.[155] These examples show that economics has become an "operational domain of warfare." [156]

U.S. military doctrine has yet to catch up. Incorporating economic tools of statecraft into operational planning will require greater technological sophistication to assess mission risk, novel mitigation strategies, and deeper cooperation between the private sector and the defense enterprise. These efforts should be housed in a dedicated entity within the Pentagon — such as the proposed Economic Warfare Operations Capability — tasked with identifying, orchestrating, and addressing fundamental risks to the industrial base and supply chains, while coordinating the interagency cooperation those missions demand.[157] There is a need to build greater trust between the private sector and the Pentagon and to teach defense leaders economic statecraft skills.

Economic statecraft lives primarily in the private sector. While the U.S. government sets the rules governing economic coercion, corporations execute the actions — and they answer to shareholders, not combatant commanders. Operationalizing economic statecraft, therefore, requires the Pentagon to cultivate closer private sector relationships and structure incentives that allow companies to profit while advancing national security objectives.

The Pentagon has already launched initiatives toward this end — the Economic Defense Unit, the Office of Strategic Capital, and the Defense Innovation Unit, among them.[158] What is missing is an integrating body that aligns these efforts toward common objectives. That is precisely the role the Economic Warfare Operations Capability could play.

Among the most acute risks to military operations is supply chain disruption. When an adversary controls the sole source of a critical component, it gains leverage over battlefield readiness without firing a shot. Tactics such as the deliberate "delaying, diverting, or destroying of an adversary's supply lines" are becoming integral to modern warfare.[159]

Vulnerabilities originate from the defense industry's multi-tiered structure, particularly for third-tier supplies and below.[160] It is at these levels where

problems, such as single sourcing, geographical concentration, and adversary origination, are typically found. Successive U.S. administrations have recognized the importance of supply chain resilience in the abstract. Yet, the Pentagon has not translated that recognition into operational planning tools that commanders can actually use.

That starts with visibility. The Pentagon cannot identify adversary chokeholds without detailed supply chain data from its contractors. However, few corporations know their full supply chain, particularly at the third-tier supplier level and below. Recent surveys show that although 60 percent of firms report comprehensive visibility into tier-one suppliers, only 30 percent report visibility further downstream, while just 17.1 percent analyze critical suppliers down to tier 4 and beyond.[161] Suppliers are often reluctant to share this information for fear of competitive exposure. In short, there are no financial incentives for sharing this information and some risk in doing so.

Addressing supply chain vulnerabilities will require both technology and leverage. AI-powered supply chain mapping can help fill informational gaps. This software is already being used in other industries.[162] There are significant limitations, however, to this approach. Christine Michienzi notes that "information obtained from this method does not come from the suppliers themselves and is usually not verified."[163] It is also "only accurate in that moment in time."[164] Moreover, AI software has been known to create "false positives" due to its reliance on public data.[165] Finally, the classified nature of some products is an additional complication to using this software in the defense industry. Therefore, software is not sufficient on its own. The Pentagon should use its purchasing power to require greater supply chain transparency from prime contractors, pairing those requirements with financial incentives and strong data privacy protections. Critically, this same analytical effort should extend to adversary supply chains. Understanding where China or others are vulnerable is essential to planning effective countermeasures.

This knowledge would also lead directly to operational planning for missions. The Pentagon would need to provide a tool that allows commanders to assess economic risks, particularly those of supply chain chokeholds that may affect equipment fielding, routine repairs, and depot-level maintenance.

Identifying risks is only half the equation. Mitigating them requires actively managing interagency investment in supply chain resilience. The U.S. government has made significant investments in critical minerals, domestic semiconductor manufacturing, and other strategic goods through the Pentagon, the Departments of Commerce and Energy, the Export-Import Bank, and the Development Finance Corporation.[166] These investments come in varied forms: loans, grants, equity stakes, and instruments like the "golden share" in Nippon Steel.[167] They lack, however, a central coordinating body. These efforts have also been fragmented, geared to a particular sector or material. This ignores the importance of interdependence between sectors.[168] Given that these efforts are justified on national security grounds, placing a coordinating function under the Pentagon is a logical step.

Mitigation of supply chain vulnerabilities also requires shifting the Pentagon's acquisition mindset. The post-Cold War fixation on lowest-cost procurement is a strategic liability when adversaries can weaponize the supply chains that lowest-cost sourcing created. The Trump administration has begun that shift through acquisition reform that emphasizes speed over cost.[169] The same logic applies to supply chain security: Companies may move to U.S. and allied suppliers if they are confident they will be compensated for the premium.

Operationalizing economic statecraft also requires better intelligence. Here, the United States faces a structural disadvantage: The availability of American financial and corporate data allows adversaries to map U.S. industries with relative ease — identifying bottlenecks, dependencies, and vulnerabilities before any shots are fired. The Pentagon and intelligence community should develop new pathways to collect economic data from U.S. firms operating in China or with significant Chinese business exposure. As Karyn Eliot and Jennifer Buss have argued, this fusion should be bidirectional — information flowing both from and to the private sector.[170] Strong data protections will be non-negotiable, as will trust. Initiatives like the recently formed Business Operators for National

Defense offer a foundation, though their mandate would need to expand well beyond acquisitions to support this mission.[171]

Trust among America's international partners is also of paramount importance. Economic statecraft is most effective when pursued multilaterally, but multilateral coalitions are inherently fragile. Trust building should happen at all levels in the chain of command. For example, combatant commanders, who maintain day-to-day relationships with partner militaries and have direct access to partner nation political leadership, are uniquely positioned to assess coalition cohesion in real time and to flag the conditions under which partners may opt out of U.S.-led economic pressure campaigns. This is intelligence in the operational sense, and it is currently underexploited.

None of this works without education. The best supply chain mapping tools accomplish nothing if commanders do not know how to use them or why they matter. Presently, few "full-time career military members and their civilian counterparts" have expertise in the tools of economic statecraft — "global markets, financial services, acquisitions processes, and proficiency in statecraft."[172] The adversary's ability to impede repairs, constrain procurement, or deny critical components is as operationally relevant as its order of battle. Military leaders at every level need to understand these risks and incorporate them into planning.

Economics and logistics have always shaped the capacity to wage war. What is new is the degree to which economic statecraft has become a primary instrument of competition — and the degree to which the United States, having hollowed out its manufacturing base over decades, is exposed to it. The military should reorient accordingly: building tools that let commanders assess economic risk, creating structures that align government and private sector action, and cultivating leaders who understand that the bombs, aircraft, and ships required for modern war are only as effective as the supply chains that sustain them.

Establishing the Economic Warfare Operations Capability, or a similar integrating entity within the Pentagon, is one concrete step toward that reorientation. It will not solve the problem on its own, but it would provide the institutional architecture around which a genuine whole-of-government economic warfare capability could be built.

Anita R. Kellogg, Ph.D., is an assistant professor at the Eisenhower School of the National Defense University. She is also the host of Kellogg's Global Politics, a podcast on current events in international affairs and U.S. foreign policy.

Editors' Note: While an epilogue was not authored for this article, the editors recommend readers to the concept paper that describes the Economic Warfare Operations Capability (EWOC), which is addressed several times throughout Dr. Kellogg's piece.

The EWOC is envisioned to gather information, develop strategies, prioritize and recommend actions, and elevate policy considerations to appropriate levels with appropriate authorities to act. All such activities already exist within the U.S. as they stand but are not presently coordinated.

The stand-alone article may be found here: https://potomacinstitute.org/steps/images/PDF/Articles/EWOCSingleJuly2023.pdf

An extended version of the paper appears in *Elements of Global Competition*, The Potomac Institute Global Competition Project, "An Operational Approach to Address Adversarial Economic Activities," Potomac Institute Press, page 81, 2023, accessible at https://potomacinstitute.org/images/gcp/gcp-compendium-final-2023-april.pdf



CHAPTER 7

ABSTRACT

Cyber statecraft and economic statecraft are increasingly intertwined in U.S. strategic competition with China. Much of contemporary economic statecraft relies on and is executed through cyberspace. At the same time, adversarial cybercrime, digital espionage, and disruptive cyber operations are imposing escalating economic costs to further strategic objectives. America's economic statecraft today faces many of the same challenges that U.S. cyber statecraft has faced for more than a decade: immature strategic formulation, barriers to public-private information sharing, and fragmented authorities.

The evolution of U.S. cyber statecraft offers key lessons for strengthening the nation's economic statecraft. For greater effectiveness, American economic statecraft must adopt a longer-term, objectives-based strategy underpinned by active and persistent economic campaigning against adversaries. Economic statecraft also requires better alignment of information sharing incentives across government and industry. The centralization of cross-departmental and agency efforts can also facilitate the execution and coordination of economic statecraft. By leveraging its experience in cyber statecraft, the U.S. can better compete with adversaries below the threshold of war and counter hostilities once they start.

Scan the QR code to view the webinar that accompanies Chapter 7.

SEEING THE CYBER IN ECONOMIC STATECRAFT

Jason Blessing

WAR ON THE ROCKS

Americans lost nearly $21 billion to cybercrime in 2025, a new record for cyber-enabled economic losses.[173] Private sector losses to malicious cyber activity regularly exceed $200 billion in a given year.[174] Alongside criminal groups, state-sponsored hackers are increasingly targeting America's pocketbook.[175] Neither the economic sphere nor cyberspace are classic terrestrial warfighting domains. Yet war is being actively waged through both realms and national cyber security is vital to the prosperity and protection of today's hyperconnected economy.[176]

China is both the greatest economic threat and the most active and persistent cyber threat to the United States.[177] Both its economic and cyber statecraft campaigns reach deep into America's government, private sector, and critical infrastructure.[178] These two efforts overlap: Cyber espionage, digital theft, and supply chain compromises are key pillars of China's strategy to undermine the U.S. economy.[179] Addressing this challenge requires marshaling economic and cyber power into cohesive, coordinated campaigns.[180]

Given the inseparable nature of modern economics and cyberspace, the future of American economic statecraft lies in lessons from the nation's cyber past. America's evolving approach to contemporary economic statecraft still suffers from strategic immaturity, information sharing barriers, and institutional fragmentation.[181] U.S. cyber statecraft has grappled with identical issues for over a decade, moving from firewalled initiatives to more coherent national collaboration. Lessons from cyber statecraft show that U.S. economic statecraft should develop new strategic paradigms, recraft information sharing incentives, and centralize disparate bureaucratic efforts.

The Intersection of Economic and Cyber Statecraft

Economic statecraft focuses on deterring, compelling, or persuading through tools like sanctions, export controls, development aid, tariffs, and investments.[182] Similarly, cyber statecraft seeks to achieve policy objectives by manipulating incentives and security around digital resources, infrastructures, and interactions.[183] This can include conducting cyber operations — the use of computer code to defend, exploit, or attack computers, networks, and their information.[184]

Both necessitate whole-of-government action and private sector coordination. Economic and cyber issues cut across bureaucracies, impacting both strategic goals and daily operations. Governments set policy, but the private sector is on the front lines carrying out day-to-day statecraft. The private sector dominates the U.S. economy: Federal spending and consumption only account for roughly 23 percent and 17 percent of the 2025 gross domestic product, respectively.[185] Private spending also dwarfs government investment in cyber-related sectors like telecommunications and infrastructures like data centers.[186] Furthermore, the private sector remains disproportionately targeted by malicious economic measures and cyberattacks.[187]

The practice of economic statecraft and cyber statecraft has increasingly converged. Much of contemporary economic statecraft relies on and is executed through cyberspace.

Nowhere is the extensive overlap clearer — and failure more catastrophic — than in the financial sector. The U.S. equities market relies on digital systems to create over $1 trillion of activity per day. The New York Stock Exchange alone digitally processes over 1.2 trillion order messages daily.[188] Within domestic banking, over 800,000 electronic wire transfers occur daily amounting to over $4.6 trillion.[189] The Automated Clearing House Network, used for direct depositing paychecks, averages roughly 141 million transactions a day totaling $368 billion.[190] International transactions rely on digital messaging through the Society for Worldwide Interbank Financial Telecommunication (better known as SWIFT) to communicate and validate payment transfer details.[191] Economies collapse without the digital tools and public-private partnerships built through cyber statecraft.

The funds and sensitive data transferred across the financial sector are also prime targets for cyberattacks. The scope of compromise is massive. For example, data breaches of JPMorgan Chase in 2014, Equifax in 2017, and First American Financial Corp in 2019 cumulatively exposed over one billion customer records.[192] By 2025, a single cyberattack cost financial institutions over $5.5 million on average.[193]

Adversarial activities by states like North Korea encompass financially motivated cyberattacks for economic ends. Digital cryptocurrency theft has allowed the Kim Jong Un regime to sidestep international sanctions and fund its nuclear weapons program.[194] For economic statecraft, cyberattacks are enablers for the theft of intellectual property, proprietary economic data, and corporate trade secrets, the damages of which have been previously highlighted in this series.[195]

Simultaneously, economic statecraft tools underpin elements of cyber statecraft. The International Emergency Economic Powers Act of 1977 and the 2015 National Defense Authorization Act give the president authority to block financial transactions and seize property of foreign individuals engaging in malicious cyber activities.[196] The U.S. government has used this authority to punish Russian election interference, the SolarWinds hack, and adversarial involvement in internet infrastructure and telecommunications companies.[197] Programs like the Department of the Treasury's Office of Foreign Assets Control Cyber-Related Sanctions and rulings from the Department of Commerce have been key to implementing presidential decisions.[198]

Economic and cyber statecraft touch on nearly every element of society, from protecting bank accounts to protecting government secrets. Due to the inextricable interdependencies between global digital markets and cyber security — and the necessity of private-public collaboration across both — the evolution of U.S. cyber statecraft holds valuable lessons for its refinement of economic statecraft.

Lesson 1: New Strategic Paradigms for More Effective Competition

Senior policymakers have yet to advance a strategic vision that clearly reimagines U.S. economic competition amidst contemporary geopolitics.[199] Instead, various departments and committees have released strategies for addressing individual elements of economic statecraft without a unified approach.[200] The result is a fragmented, short-term approach to economic security that lacks a comprehensive direction for longer-term competition.[201]

Much like economic statecraft today, America's early strategic approach to cyberspace lacked a unified vision for ongoing competition with adversaries.

Slow to recognize the risks of adversarial threats, early strategies cast cyberspace as a balance between the promises and vulnerabilities inherent in new information technologies.[202] The first national cybersecurity strategy in 2003 and subsequent documents advanced this framing with little emphasis on adversaries.[203] While the Department of Defense named cyberspace as a warfighting domain in 2011 and acknowledged the threat of external actors, it received no more attention than insider threats or supply chains.[204]

Instead of defining clear tools, roles, and authorities for competition, cyber statecraft of the 2000s and early 2010s defaulted to self-restraint, nuclear-style deterrence logics, and the case-by-case response to cyber incidents.[205] Direct confrontation and sustained competition with adversaries in and through cyberspace was the exception, not the norm.[206]

As a result, U.S. cyber statecraft relied on individual departments and agencies to deploy respective economic, diplomatic, and legal means for addressing security concerns arising from adversaries.[207] Deterrence thinking prevailed but was consistently undermined by threat actors. Deterrence hinges on reliably and systematically imposing costs on attackers or reducing or denying their potential gains.[208] This is nearly impossible in cyberspace, where attackers face multiple avenues for compromise with few risks, particularly with lower-cost techniques like ransomware.[209]

Today's economic statecraft looks the same: A reactive, piecemeal approach of disparate and episodic experimentation with individual policy tools without a catalyzing vision.[210]

For cyber statecraft, 2018 marked an important turning point.[211] The Department of Defense and U.S. Cyber Command redefined the competitive landscape through two strategic concepts. In 2018, the Department of Defense introduced the "defend forward" concept, whereby the United States would "disrupt malicious cyber activity at its source."[212] Cyber Command's framework of persistent engagement operationalized the concept, further shifting U.S. posture from crisis response to active campaigning through ongoing, preemptive cyber operations.[213]

This pivot away from restraint and deterrence advanced a new strategic paradigm: Proactive cyber operations paired with private sector and allied engagement to deny, degrade, disrupt, or destroy adversarial cyber threats below the threshold of armed conflict.[214] The national cyber strategies of 2023 and 2026, along with the Defense Department's 2023 Cyber Strategy, reinforced the vision to leverage out-of-network operations for disrupting malicious actors.[215]

Greater military and law enforcement initiative has become an increasingly important prong of cyber statecraft alongside more traditional defensive measures like the "Shields Up" and "Shields Ready" programs of the Cybersecurity and Infrastructure Security Agency.[216] Economic statecraft today has no emphasis on active and sustained campaigning to gain and maintain strategic advantage.

American economic statecraft is at an inflection point where a paradigmatic shift in strategy could create a more comprehensive approach to maintaining competitive advantage. The United States should formulate a longer-term, objectives-based strategy underpinned by active and persistent economic campaigning against adversaries.

Economies collapse without the digital tools and public-private partnerships built through cyber statecraft.

Lesson 2: Changing Incentive Structures for Information Sharing

Effective economic statecraft requires information sharing between government and the private sector. Each has important insights that contribute to a competitive economic edge. However, as Karyn Eliot and Jennifer Buss highlight, there are numerous barriers.[217] National security intelligence and corporate America remain siloed: Existing incentives and practices have led to fragmented, transactional information sharing.

The same was true for cyber information sharing prior to 2015.[218] Public-private information sharing at the time occurred through the Department of Homeland Security's Office of Intelligence and Analysis and the National Protection and Programs Directorate (the predecessor to the Cybersecurity and Infrastructure Security Agency). Although not formalized until 2014, both possessed authorities for information and intelligence sharing between the government and private sector.[219]

Yet, the private sector was highly averse to sharing threat information.[220] Companies feared shared cyber intelligence might spur regulatory investigation or appear as evidence in regulatory action.[221] They also feared that proprietary or embarrassing information included in intelligence might become public through Freedom of Information Act mechanisms.[222] Companies further worried the federal government could waive intellectual property rights associated with shared intelligence concerning stolen proprietary data or trade secrets.[223] Corporations expressed broader concerns that volunteering cyber information to the government might violate privacy laws and that commercial-to-commercial sharing might result in liability over negligence, violate fiduciary and privacy obligations, or appear as coordinated anti-competitive actions.[224]

Information sharing for economic statecraft faces these same disincentives today.[225] Legislation was key to remedying these barriers for cyber statecraft, but Congress has yet to craft a solution for economic statecraft.

The Cybersecurity Information Sharing Act of 2015 greatly reshaped these incentives.[226] It advanced key definitions for 18 information sharing concepts.[227] This common set of terms facilitated information sharing agreements and laid the groundwork for subsequent efforts to clarify incident reporting standards.[228] The Department of Homeland Security became the official hub for public-private sharing and for distributing information to other departments coordinating sector-specific cybersecurity. The law also included provisions for Information Sharing and Analysis Organizations to facilitate cyber threat information sharing among voluntary members.[229]

The law established the federal government's "duty to share" with the private sector, creating a default posture of information flow instead of one concerned about intelligence gains or losses. It also limited federal uses of information for defending against cyber threats or in response to threats like terrorist attacks or serious economic damages.[230]

For private companies, it implemented cyber intelligence sharing protections, including exemptions from regulatory and antitrust enforcement, limiting disclosures under the Freedom of Information Act, and the retention ownership over proprietary information.[231]

Similar legal changes are necessary for economic statecraft efforts. Without changing incentive structures, the government and private sector face an uphill battle in sharing and acting on economic threat information.

Lesson 3: Bureaucratic Centralization Solves (Some) Problems

Economic statecraft responsibilities are spread across federal bureaucracy, making coordination an imperative. As William Norris lays out in his article in this series, more than 1,400 offices across 13 departments and 10 federal agencies have roles relevant to economic statecraft.[232]

Likewise, cyber statecraft is dispersed across the federal government, with over 500 organizations in the Department of Defense alone responsible for

elements of cyber operations.[233] Agencies necessarily possess different responsibilities and interests for executing cyber statecraft, and conflicts continue to arise as they compete for resources and power within and across administrations.

Yet, in contrast to economic statecraft, America's cyber statecraft has produced three examples of centralization that streamlined national efforts: The creation of the Cybersecurity and Infrastructure Security Agency, U.S. Cyber Command, and the National Cyber Director.

The establishment of the Cybersecurity and Infrastructure Security Agency in 2018 under the Department of Homeland Security was a watershed moment for civilian bureaucracy.[234] After the globally devastating WannaCry and NotPetya ransomware attacks of 2017, officials moved to centralize and accelerate incident response and information sharing.[235] The new agency to lead cybersecurity programs, operations, and polices and to coordinate security, resilience, and technical assistance efforts across federal and nonfederal entities.[236]

Subsequent consolidation removed redundancy and facilitated more effective coordination. The agency combined stakeholder coordination arms into a single division and created a common communication hub for critical infrastructure partners.[237] It also unified three different operations centers for information sharing and incident response to enhance awareness and threat monitoring.[238] Despite its successes coordinating national cybersecurity, the agency faces a drastically reduced role under the current administration.[239] The Trump administration has made extensive cuts to the agency's election security, stakeholder engagement, and broader workforce with an eye towards dramatically reducing its budget.[240]

The creation and elevation of U.S. Cyber Command streamlined the coordination and expansion of military cyber operations.[241] Prior to 2010, those activities were relegated to different joint task forces housed at different times under various Department of Defense organizations.[242] The 2008 Agent.BTZ compromise of the Defense Department's secret computer network showed the need to centralize and coordinate military cyber resources.[243]

U.S. Cyber Command has since provided a unity of command and mission clarity for protecting defense networks and executing cyber operations in service of policy goals. Additionally, because one individual leads both U.S. Cyber Command and the National Security Agency the Department of Defense can assess and mitigate the tradeoffs of disrupting or continuing intelligence collection on an adversary.[244] The 2018 elevation of U.S. Cyber Command to a standalone combatant command served to attract greater resources and coalesce coordination to combat adversarial cyber threats.[245]

Economic statecraft lacks similar bureaucratic and policy focal points for information flow and stakeholder coordination. Responsibilities remain primarily split among the Departments of Treasury, Commerce, State, and Defense, with no partner leading the dance.[246] A new agency is not the only answer, but effectively coordinating economic statecraft mandates a more permanent solution than temporary, issue-driven interagency committees. The Office of Strategic Capital within the Department of Defense has helped to centralize and scale investments into critical technologies but it has limited coordination ability vis-à-vis other federal departments outside the Department of Defense.[247]

At a higher executive level, Congress established the Office of the National Cyber Director and confirmed the first National Cyber Director in 2021 to better galvanize and coordinate cyber statecraft.[248] Centralizing executive branch leadership was a necessary step to align interagency planning, resourcing, implementation of federal cyber policy and strategy.[249] The Office has since played a central role in developing and implementing the 2023 and 2026 national cyber strategies and the first strategy for improving the national cyber workforce.[250] More broadly, the Office has worked to strengthen interagency, public-private, and international coordination on key U.S. interests related to cyberspace.[251]

A new strategic office or organization is also necessary to align, coordinate, or deconflict the diverse elements of economic statecraft. Any new bureaucracy should also be fit for purpose — reorganization for the sake of reorganization is unlikely to beget increased competitiveness vis-à-vis economic adversaries.

At the same time, the U.S. government should deal with the growing pains a new economic statecraft bureaucracy will inevitably face. For instance, in addition to political pressures, the Cybersecurity and Infrastructure Security Agency remains hamstrung amidst ongoing structural changes, slow response times, and inconsistent engagement practices.[252] U.S. Cyber Command did not eliminate bureaucratic turf battles, and the command still struggles with fragmented command and control over its subcomponents.[253] The Office of the National Cyber Director lacks performance measures and cost estimates for its strategic initiatives, struggles to determine and allocate resources, and has no true enforcement power.[254]

Learning from Cyber: The Way Forward for Economic Statecraft

America's evolving cyber statecraft, and its corresponding institutions and processes, provide a series of lessons upon which U.S. economic statecraft can build for future success. While challenges for cyber statecraft still remain, the increasing interdependence and overlap between economic statecraft and cyber statecraft necessitate learning from the recent past.[255]

U.S. cyber statecraft has grappled with the same strategic, informational, and bureaucratic challenges facing economic statecraft today. Getting economic statecraft right also bolsters cyber statecraft. The two are interdependent and mutually reinforcing, and the global competitive environment requires leveraging economic and cyber efforts in tandem.[256]

America has all the right tools for conducting effective economic statecraft, and now is the time to integrate them with novel strategy, new incentive structures, and more streamlined coordination.

Jason Blessing, Ph.D., is a Research Fellow at the Potomac Institute for Policy Studies. His research focuses on the intersection of cybersecurity, defense policy, and international relations. All views are his own and do not represent the views of the Institute.

Economic and cyber statecraft touch on nearly every element of society, from protecting bank accounts to protecting government secrets.

CHAPTER 6 EPILOGUE: THE IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

Jason Blessing

The growing importance of artificial intelligence (AI) further highlights the convergence of cyber statecraft and economic statecraft. AI models are becoming both powerful enabling tools and strategic terrain for competitive statecraft efforts, with U.S.-China competition at center stage. Competition increasingly covers the entire AI technology stack, including computer chips, servers, data centers, software, data, models, applications, and other elements of the AI ecosystem.

Gaining and maintaining advantage in AI-related markets, to include developing and securing the latest-and-greatest AI models, [257] provides powerful leverage for economic statecraft and economic security. Frontier models, which represent the leading edge of AI capability at a given time, are increasingly at the heart of AI-focused competition. Unlike foundation models, which focus on narrow tasks through basic pattern matching and summarization, frontier models are capable of complex, multi-step logical reasoning and can handle tasks for which they were not specifically trained to execute. Additionally, while the trained parameters of foundation models tend to be publicly published (i.e., open weights), most frontier models remain more secretive with closed weights, restricting access and insight to proprietary parameters.[258] Critically, frontier models also require specialized servers and data center infrastructure that expand the scope of economic competition.

AI models are accelerants for both cyber and economic statecraft. For cyber operations, AI can reduce operational costs, condense timelines, and expand scale. For cyber defenders, AI can facilitate faster vulnerability scans, implement adaptive authentication measures and scale the analysis of threat intelligence to identify potential intrusion campaigns. In offensive cyber operations, adversaries like China, Russia, Iran, and North Korea are already using AI[259] to code and enable malware, translate foreign languages, analyze stolen data, and mass-generate social engineering content.[260] Recent training mishaps at both OpenAI and Anthropic — where respective models escaped testing environments to hack into the networks of other companies — show the ability of frontier models to identify and exploit vulnerabilities at scale and speed.[261] The exploitation of AI presents staggering potential for strategic advantage.

On the economic front, global corporate investment in AI has skyrocketed, reaching $581.69 billion in 2025 — a nearly 130 percent increase from 2024.[262] For invested nations, this makes AI a point of strategic leverage. In the United States, AI-related companies have added roughly $27 trillion in market value since 2022.[263] AI is already being used to write and review code, automate customer service, enhance medical imaging and diagnostics, accelerate drug discovery, optimize supply chain logistics, and manage transportation networks.[264] The financial sector heavily leverages AI models for credit underwriting, personalized banking, and in cybersecurity and anti-fraud operations to assess anomalous transaction behavior, identity verifications, and network relationships.[265] The anticipated cost-savings of AI across the U.S. economy — particularly in service operations, supply-chain management, software engineering, and strategy and finance — are projected to increase U.S. productivity and GDP by 1.5 percent by 2035.[266]

Growing economic dependencies on and expected economic benefits of AI make models and their enabling technologies increasingly powerful choke points for crippling adversarial competitiveness. For instance, AI technology restrictions hinder the ability of adversarial militaries to train and use frontier models for applications like military simulation, intelligence processing, surveillance, and weapons design. AI models themselves are also novel targets. Adversarial cyberattacks seek to steal and exploit training or operating data, user information, model

weights, retrieval systems, and administrative permissions for unauthorized action.[267]

As a result, competition over AI models and their technology stacks heightens the need for more robust strategic formulation, information sharing incentives, and bureaucratic responsibilities.

Unfortunately, America's current AI strategy is marked by political whiplash between rapid deployment and safety. Stated goals include promoting innovation, building out domestic AI infrastructure, setting standards for evaluating national security risks of frontier models, and exporting American AI to allies while strengthening export controls for the AI stack.[268] Yet, strategy in action has been plagued with the same reactive, episodic approach that has marked America's recent economic statecraft.

For example, in May of 2026, the Pentagon blacklisted Anthropic and its models over ideological differences about AI safety.[269] Then, on June 12, 2026, the Department of Commerce abruptly imposed export controls on Anthropic's latest Claude Mythos and Claude Fable frontier models after deeming them too dangerous for all foreign users.[270] No exemptions were made for U.S. allies. Building on Executive Order 14409 from June 2026, the White House is now moving to formalize a voluntary framework for evaluating closed-weight, state-of-the-art frontier models that carry national security risks. Open models are currently excluded from review. However, the framework will remain nonpublic and reportedly has no clear criteria for defining national security risk or what constitutes state-of-the-art capability.[271]

The broader concern is that such a review framework creates a *de facto* AI strategy that does not align with the United States' emergent economic statecraft strategy. Secretary of the Treasury Scott Bessent's recent articulation of strategy[272] begins to lay out a long-term, proactive approach for persistent economic competition with adversaries. However, restricting frontier AI models, with little justification of the tangible national security threats posed, runs counter to advancing innovation and leading markets.[273] When access to U.S. frontier models is shut off,[274] it cedes an opening for Chinese AI models like Kimi K3 to capture larger market shares and set international standards.[275] At the same time, the current focus on frontier models risks de-emphasizing the role that smaller, specialized foundation models can play in helping the U.S. establish analytic superiority over its adversaries.[276]

For AI-centric economic statecraft, information sharing problems remain even more acute than for more general economic statecraft efforts. In theory, AI should facilitate better economic intelligence, compliance audits, and information sharing through the speed and scale of computing power. However, companies maintain few motivations for sharing information about models themselves. For instance, the private sector lacks incentives for disclosing either prompt-based attacks that cause AI models to circumvent safety features ("jailbreaks") or unauthorized escapes from AI model training environments ("sandbox escapes"). While federal security guidance exists,[277] there are no reporting requirements. Without legal obligation, company decisions to self-report incidents will inevitably be tied to liability and financial considerations.[278]

AI governance for economic statecraft is also likely to strain and exacerbate the existing bureaucratic issues still facing broader economic statecraft: fragmented authority, information flow, and lack of unity of effort. The Departments of Commerce, Treasury, Homeland Security, Defense, State, and the White House are all likely to have legitimate equities in reviewing the national security implications and export risks associated with frontier models. Yet, the Trump administration's proposed frontier model review process will include various administration officials rather than a single office or agency. This has the potential to worsen bureaucratic coordination and complicate ownership over AI as a tool of economic statecraft.

AI presents both a powerful tool and a complicating element for American economic statecraft. AI models and the AI technology stack provide critical leverage for influencing and shaping economic competition. At the same time, utilizing and protecting AI faces the same strategic, information

sharing, and bureaucratic issues encountered by broader U.S. economic statecraft. Policymakers must ensure that America's AI strategy aligns to its emergent vision for economic statecraft. Getting AI right has the potential to give the U.S. unprecedented economic advantage over competitors like China, while fostering a foothold for enduring security and prosperity.

Jason Blessing, Ph.D., is a Research Fellow at the Potomac Institute for Policy Studies. His research focuses on the intersection of cybersecurity, defense policy, and international relations. All views are his own and do not represent the views of the Institute.



CHAPTER 8

ABSTRACT

Global commercial systems and institutions are increasingly being weaponized to employ coercive economic statecraft. As supply chains, financial infrastructure, energy and communication systems, and technology ecosystems all become grounds for power competition, and strategic and operational risks faced by the U.S. and American firms converge, a more integrated strategy to combat economic pressures is in demand.

Gen. Ray calls upon corporate executive teams and boards to redefine their standards of corporate stewardship to better reflect the current strategic risk environment. Deliberate alignment and dialogue between Congress, the military, and industry is conducive to a more effective policy environment and U.S. response to economic statecraft. From there, a broader national security industrial base can develop to better withstand coercive economic statecraft and deter adversarial efforts through resilience.

Scan the QR code to view the webinar that accompanies Chapter 8.

RETHINKING CORPORATE RISK AND ALIGNMENT IN AN ERA OF ECONOMIC STATECRAFT

Gen. (ret.) Timothy Ray

In Sept. 2010, following a collision between a Chinese trawler and Japanese coast guard vessels near the Senkaku Islands, Chinese authorities halted shipments of rare earth minerals to Japan.[279] The move disrupted supply chains for everything from consumer electronics to advanced defense systems, driving immediate shortages and cost spikes.

At the time, many treated the episode as a discrete diplomatic flare-up. In retrospect, it was an early demonstration of something larger: that economic interdependence could be weaponized, and that the systems underpinning global commerce were becoming instruments of strategic competition.

When I joined Business Executives for National Security as CEO two and a half years ago, following a career in the U.S. Air Force that culminated in commanding Air Force Global Strike Command, I thought I understood the challenge. Like many who have spent their careers in government and uniform, I assumed much of the task would involve reconnecting business leaders to national security risks they had grown too distant from and helping the government understand more effective tools used in the private sector. The implied theory of change was straightforward: Government defines the problem and the private sector helps deliver the solution.

I have since come to think that diagnosis is incomplete — not because it misidentifies the problem, but because it misidentifies the nature of the relationship now, in an era increasingly defined by economic statecraft.

Over years of conversations with business leaders, I have come to understand that many are working from a strategic model that does not fit with the risks, exposure, and pace of this environment. In a world shaped by globalization and the assumption that commerce and stability reinforced one another, broad geopolitical risk was not understood to fall within the ordinary scope of fiduciary responsibility.

That environment has changed. In a logic reminiscent of the Cold War, the United States has reentered a period in which economic endurance and stability is central to national security. Today, the terrain of competition runs through supply chains, energy systems, financial infrastructure, communications networks, and technology ecosystems. Private firms are instruments and arenas of that competition, operating directly on the front lines. They are not indifferent to the risks, to be clear, but they lack the full story of what's at stake and the resources and knowledge to understand how to respond.

This new environment does not require firms to adopt a foreign policy agenda or subordinate commercial judgment to government priorities. It requires something more practical: a recognition that the strategic risks now confronting the United States and the operational risks now confronting American firms are increasingly one and the same. A shared understanding of that exposure is the only foundation on which a serious response, from the U.S. government and private sector alike, can be built.

How Economic Interdependence Became Strategic Leverage

For most of the postwar era, the alignment between American commercial and strategic interests could be taken largely for granted. The United States built the modern international economic order — Bretton Woods, the dollar-denominated financial system, the architecture of global trade — and the rules of that system reflected and reinforced American power. Firms pursuing profit within it were, in a meaningful sense, also reinforcing the structure that protected them. The assumption underlying this era of increasing globalization was that economic interdependence, including the integration of China into the global economy, ran in roughly the same direction as American interests.

That assumption no longer holds. The United States is no longer the most effective actor wielding economic tools to achieve its strategic ends. Competitors, most notably China, are applying economic pressure in ways that are often more opaque, more targeted, and more integrated with national strategic objectives.[280] American firms that have built their strategies around the assumptions of the prior era will find themselves caught between foreign economic coercion on one side, and a U.S. policy environment increasingly oriented toward de-risking, friend-shoring, and the reconstruction of domestic industrial capacity on the other.

The telecommunications industry shows most clearly what happens when one side figures that out before the other.

The United States invented cellular technology and — along with allied firms — led telecommunications infrastructure for decades. That position eroded over the course of two decades not because American firms were out-innovated, but because they played by the rules of the existing commercial market: If firms remained competitive on commercial terms, the national interest would take care of itself.[281]

China operated from a different premise. For Beijing, telecommunications was a strategic industry tied directly to technological sovereignty, industrial power, and long-term geopolitical leverage. Subsidized by the state, provided with cheap credit, and shielded from the normal disciplines of competition through protected access to the state market, Huawei was able to both absorb Western technology and vastly undercut global market prices. Beijing extended this advantage beyond Huawei's own balance sheet, as state-owned lenders extended billions in financing directly to Huawei's customers, effectively making it easier for foreign buyers to choose Huawei over any Western alternative.[282] Huawei, accused by the U.S. government for years of constituting a possible security risk, now holds roughly 30 percent of the global market — a larger share than the next most popular vendors, Nokia and Ericsson, combined.[283]

The failure here was not that American firms were uniquely incompetent or that American engineers were outclassed. Many of these companies were highly capable and, in narrow business terms, often acting rationally. But decisions that were individually rational inside the commercial logic of the time — offshoring production, competing aggressively on cost, prioritizing financial efficiency over manufacturing depth — became collectively corrosive when applied inside a contest that was never purely commercial to begin with. The problem was that they were operating within a strategic framework that no longer matched the environment, while their principal competitor was operating within one that did.[284]

The Case for Redefining Corporate Self-Interest

Ten years ago, it was still possible to argue that parts of the American business community were naive about China's motives, methods and long-term strategic ambitions. That is much less true today. In my experience, few business leaders are under any illusion about the nature of the Chinese system or the risks of deep dependence on it. What many are wrestling with is not recognition, but response.

Untangling from China is not a matter of simply waking up and walking away. For many firms, it is a board-level decision governed by legally binding fiduciary obligations, supply chain realities, sunk capital, customer exposure, and the practical limits of how quickly production can be relocated without damaging the enterprise itself.

The range of private sector responses reflect that reality. Some firms have concluded they will remain until the environment becomes untenable.[285] Others want to reduce exposure but cannot do so responsibly without a viable alternative.[286] Still others are actively moving, only to find that unwinding years of integration takes years more.[287]

The strategic problem, then, is no longer primarily one of awareness. It is that many firms remain structurally entangled in a system they increasingly understand to be risky and lack a clear framework for thinking about what responsible adaptation actually requires. Washington will eventually have to build that framework, but firms cannot afford to wait for it to be finished before they begin to act.

That adaptation starts with redefining corporate self-interest. The central question is no longer simply what maximizes efficiency under stable conditions. It is what protects the long-term viability of the enterprise in an environment where geopolitical exposure and strategic dependency increasingly shape business outcomes. For most boards and executive teams, this does not require an entirely new way of thinking: It requires expanding familiar categories of risk to reflect the environment as it actually exists.

Four of those categories deserve particular attention.

The first is input dependency. If a firm relies on a single region, supplier base, refining process, software stack, or politically exposed market for inputs it cannot easily replace, it needs to move beyond asking if the dependency is profitable under normal conditions, but whether it is tolerable under stress.

The second is market access as leverage. A company that builds deep revenue dependence in a market where access can be restricted as an instrument of statecraft has a pressure point that can be used not only against the firm, but against broader U.S. policy choices in moments of crisis.

The third is infrastructure and ecosystem concentration. As competition increasingly runs through the systems on which commerce depends — communications hardware, cloud architecture, logistics nodes, and energy reliability — dependence on infrastructure becomes a material strategic liability. The issue is no longer simply who your customer is or where your factory sits, but what larger system you are implicitly betting the enterprise on.

The fourth is time horizon, which relates implicitly to each of the above considerations. Some parts of the private sector already manage this well — banks, insurers, and internationally exposed firms often have more developed instincts for political and systemic risk. But that adjustment is far from universal. In many other firms, greater analysis and strategic inquiry are still needed to properly incorporate the broader risk environment into the enterprise's overall calculus. The issue is not simply the pace of decision-making, but whether the firm is fully accounting for the strategic trends and systemic exposures that increasingly shape its operating environment.

None of this means firms must subordinate commercial judgment to government direction or treat national objectives as a substitute for fiduciary duty. It means the opposite: Boards and executive teams should update their own definition of prudent stewardship to reflect the strategic environment. The market — for now — does not consistently price these risks, which is why firms cannot wait for market signals to tell them when recalibration is necessary. The firms that adapt fastest will be the ones that understand where strategic risk sits inside their own business model and move early enough to preserve optionality before events remove it for them.

The Three-Party Problem

None of that adaptation happens in isolation. Every significant investment, industrial commitment, or supply chain decision of strategic consequence ultimately requires a stable and predictable policy environment — one that only Congress can fully provide. That makes the broader relationship and alignment between Congress, the military, and industry foundational to America's response to economic statecraft.

When the relationship between these three entities works in harmony, the results are visible. One of my last roles in the Air Force was overseeing the acquisition of the B-21 Raider. The B-21 is both

on schedule and maintaining unusual cost discipline — an outcome rare enough in major defense acquisition to surprise even seasoned observers.[288] The success of the programs is a direct result of Congress, the Air Force, and the relevant prime contractors maintaining genuine alignment: shared visibility, shared tolerance for risk, and clear prioritization, with everyone in the same room solving the same problem.

The challenge today is that the terrain of competition has expanded well beyond the traditional defense industrial base, while the mechanisms through which all three parties interact have not kept pace. Closing that gap is a shared problem.

For Congress, it means developing visibility into how modern firms actually allocate capital and assess risk to ensure that policy is grounded in how these systems work in practice. Incentives, tax structures, and capital formation mechanisms need to be oriented toward long-term productive capacity and national security interests, not just short-term efficiency. Permitting and regulatory timelines should be reconciled with the speed at which strategic competition is unfolding. For the military, it means translating operational requirements into terms that connect clearly to the commercial ecosystems on which readiness increasingly depends. For industry, it means engaging with transparency about where dependencies exist, how long transitions take, and what tradeoffs are unavoidable. And, for all three actors, it requires a more deliberate and sustained dialogue — rather than episodic engagement during crises — grounded in shared exposure to strategic risk.

Congress is, after all, the closest thing this government-industry partnership has to a corporate board. It sets the conditions — through policy, incentives, and capital — on which the entire three-party alignment depends. When it is a well-informed partner, the system functions. When it isn't, Congress risks exercising authority without sufficient visibility into the systems it is trying to shape.

Resilience as Deterrence

Neither the scale nor the complexity of these challenges should be cause for fatalism. Americans have a habit of rising to meet moments like this one. The architects of the post-World War II economic order were not responding to a world they fully understood, but they nonetheless built forward, leveraging American economic weight, industrial ingenuity, and institutional confidence to shape a system that reflected U.S. interests and values. The task now is not to replicate that era, but to recover the strategic discipline that made it possible.

What that discipline produces, when firms and government develop a genuinely shared picture of the strategic environment, is a national security industrial base broad enough to reflect how power is actually generated — and protected — in this age of economic statecraft.

That broader understanding rests on three mutually dependent pillars. The first is the classic defense industrial base: the specialized capacity to produce munitions, submarines, combat aircraft, and missile defense, and the industrial depth required to sustain military operations over time.

The second is the dual-use technology and manufacturing base, where the most strategically consequential capabilities of this era are emerging and scaling. Software, autonomy, microelectronics, advanced manufacturing, and AI-enabled tools may not originate inside the traditional defense sector, but they are increasingly central to military advantage and economic power alike. They are best generated not through tightly managed government structures, but through a dynamic private sector capable of moving faster, iterating more rapidly, and scaling in ways the traditional defense system often cannot.

The third is resilient infrastructure, the physical and digital systems on which both pillars depend. This includes energy grids, ports, logistics networks, communications architecture, cloud infrastructure, and undersea cables. They are the connective tissue that allows the other two pillars to function at all.

None of these pillars stand alone. A world-class defense industrial base without dynamic dual-use innovation becomes too narrow, too slow, and too expensive. A vibrant technology sector without resilient infrastructure remains exposed and brittle. Infrastructure alone, no matter how hardened, cannot substitute for either. Each depends on the others — which is precisely why the alignment between firms and government matters as much as any individual investment or policy. And that alignment has to hold not just in periods of competition, but also under targeted, adversarial pressure.

That pressure is not abstract. For much of the post-Cold War era, the United States operated as though the homeland could be treated as a secure rear area: a stable base from which power could be projected without meaningful contestation. That sense of sanctuary is increasingly under duress. Adversaries now have multiple ways to impose costs and generate pressure well below the threshold of conventional attack through economic coercion, supply chain disruption, and sustained pressure against these three pillars, on which military readiness and economic continuity depend.

The same vulnerabilities that leave companies vulnerable to missing their profit margins are those that threaten U.S. security at home. An adversary that believes it can impose enough economic pain to limit U.S. options is a credible threat to U.S. security — in addition to firms that would be the first-order victims.

In that environment, resilience is not only a defensive virtue, but also a strategic signal. A country that can absorb disruption, maintain production, and keep its private sector functioning under pressure is harder to coerce and less likely to be tested in the first place. Deterrence, in this sense, now includes deterrence by resilience: not just the capacity to prevail in a fight, but the demonstrated ability to absorb economic pressure without altering course.

The objective is not to "out China" China, or to replace the dynamism of the American private sector with a centrally planned alternative. It is to recognize that the United States now needs a national security industrial base broad enough to reflect how power is generated in this century and resilient enough to endure the kinds of pressure that will increasingly define strategic competition.

If shared strategic risk is the foundation for a new alignment between government and business, then deterrence through resilience is the condition that allows that alignment to hold under stress. Without it, the very systems on which American power depends become vulnerable to coercion before a crisis ever becomes a war.

Gen. (ret.) Timothy Ray is the chief executive officer of Business Executives for National Security. He last served as the commander of the Air Force Global Strike Command and Commander of Air Forces Strategic-Air, U.S. Strategic Command.

Private firms are instruments and arenas of that competition, operating directly on the front lines.

CHAPTER 8 EPILOGUE: FROM RISK TO REINVESTMENT

Gen. (ret.) Timothy Ray

When I wrote "Rethinking Corporate Risk and Alignment in an Era of Economic Statecraft," my objective was to encourage business leaders to reconsider the strategic environment in which they operate. Geopolitical competition has changed, and the assumptions that shaped corporate risk management for much of the post-Cold War period no longer fully reflect the realities confronting American companies or the nation they support.

Mark Rosenblatt's contribution to this series, "Rebuilding American Manufacturing: A Keystone for Economic Statecraft," picks up a thread my article left open.[289] If companies are expected to account for geopolitical risk differently, what conditions make those investments commercially sustainable and consistent with the fiduciary duty of the profit-interested boards I sought to motivate? His answer is refreshingly specific: he suggests the government carry its share of the cost. And this matters enormously to my premise, because a shift in corporate risk thinking cannot rest on asking firms to absorb the costs of such a transition unilaterally. Creating the structural conditions that let a board act on an updated perception of risk without treating it as an act of self-sacrifice against its shareholders is a natural and supportive complement to the governance question I raised previously.

My piece asked how boards should weigh risk, while his asks what has to be true for that updated thinking to translate into investment. Rosenblatt also helpfully details the industrial policy layer, asking the critical question of what makes manufacturing investment viable. Together, these questions create a logical confluence of thinking. A board's updated risk appetite means little without the capital and policy conditions to act on it; conversely, those conditions mean little to a board that hasn't updated how it thinks about geopolitical exposure in the first place.

Underneath both of our arguments sits a concern common to both of our articles, but one I think critical to the discussion: durability. Rosenblatt's mechanisms only change a board's math if firms can count on them holding for the life of the investment, not just the life of a single year's appropriation, an isolated policy, or even a specific Congress or Presidential administration. The governance shift I called for works the same way — a board can change its definition of prudent stewardship, but should only do so if the signals to which it is responding are stable enough to underwrite a decision measured in years or decades. Durability here — or bankable predictability — isn't a separate variable from incentive design. It's a precondition that makes incentive design worth anything.

This is why I framed economic statecraft as a three-party problem: industry, the military, and the government each playing a distinct role, with the latter necessarily providing the legislative durability that gives strategic priorities staying power. Rosenblatt's piece makes that role concrete: durability is the specific, patient work of writing incentive mechanisms into law with enough permanence that a bank underwriting a manufacturing loan, or a board underwriting a supply chain redesign, can treat them as fixed points. That's a standing invitation to the national security leaders in Congress and the White House: the most valuable thing you can supply industry right now isn't a new mandate, it's predictability. Fund the mechanisms, then hold the line on them across budget cycles and administrations. This may be easier said than done, I know. In the last thirty years (1996–2026), a full Defense Appropriations Act has been passed prior to the start of the Fiscal Year exactly seven times.[290] These delays block the Pentagon from starting new acquisition programs or increasing production rates. And for private-sector defense contractors, this creates revenue unpredictability, delays contract awards, and forces inefficient short-term

production planning that inflates costs for supply chains. Abrupt policy changes, too, can complicate procurement and spending downstream, further muddying already turbulent waters.

The B-21 bomber program succeeded on exactly the kind of consistency and durability, sustained across successive administrations, that may be in systemic short supply. But it shouldn't be. Industry can't manufacture that predictability on its own, nor can all the funding in the world simply create it from whole cloth. Only concerted effort by Congress and the White House, acting together and staying the course, can supply it.

Rosenblatt's essay is the ninth entry in this series' effort to map how the United States should organize economic statecraft; mine was an earlier one, focused on the firm rather than the industrial base. I'd like to think they're in conversation with each other in the way the series intends, each sharpening the other. His concrete mechanisms give texture to my case for updated fiduciary thinking, while my case for board-level engagement gives Rosenblatt's manufacturing incentives a constituency, and my three-party framing gives both of us a place to direct the request for durability: to the leaders in the military, Congress and the White House who control the landscape.

After all, economic statecraft, in the end, is not something government does to the private sector, or something industry volunteers for government. It is a shared architecture that is funded, legislated, and durable, and a space within which commercial judgment and national interest can (and ideally, should) point the same direction. The B-21 remains a useful illustration of what that alignment looks like when it works. Whether it becomes the exception or the rule will depend on whether we keep building the kind of durable partnership Rosenblatt describes for manufacturing, and that I hope to see extended into national security-minded corporate decision-making.

Gen. (ret.) Timothy Ray is the chief executive officer of Business Executives for National Security. He last served as the commander of the Air Force Global Strike Command and Commander of Air Forces Strategic-Air, U.S. Strategic Command.

Durability here — or bankable predictability — isn't a separate variable from incentive design. It's a precondition that makes incentive design worth anything.

CHAPTER 9

ABSTRACT

Decades of offshoring has hollowed out American manufacturing and left the country dependent on China; U.S. reliance on Chinese imports has inadvertently bankrolled China's burgeoning innovation, manufacturing, and technology sectors. Manufacturing competitiveness on the global stage, is foundational to a nation's wield of economic statecraft as a strategic tool. To that end, matching China's manufacturing depth across industries will take sustained rebuilding at home combined with cooperation among traditional allies and partners.

The article frames the choice plainly: rebuild critical domestic manufacturing or remain dependent on China, risking U.S. prosperity and security. Rebuilding starts with AI-optimized production, encouraged through a framework of policy incentives that sidestep "picking winners." A reshoring agenda would strengthen manufacturers' income statements through transferable tax credits, drive investment in domestic capacity at scale, and reward manufacturing entrepreneurship as an American asset through a capital gains exemption program. Bottom line, manufacturing competitiveness is the precondition for every other instrument of American power, to include effective economic statecraft.

Scan the QR code to view this article on the Potomac Institute for Policy Studies website.

REBUILDING AMERICAN MANUFACTURING: A KEYSTONE FOR ECONOMIC STATECRAFT

Mark Rosenblatt

In September 2010, after a Chinese fishing trawler captain was detained near the Senkaku Islands, Beijing halted rare-earth exports to Japan.[291] The embargo lasted weeks. China showed, on a U.S. treaty ally, how a supply chain could be weaponized. Washington failed to respond.[292] Nor did America generalize the lesson. Instead, it benefited from deflation as it increased its dependency on China over the past 20 years.[293] The number of Chinese companies exporting into the U.S. manufacturing supply chain rose from 10,500 to 39,000 from 2005 to 2024.[294]

China's rare earths actions are just the tip of the spear — the shaft is now coming through the bulwarks.[295] High quality Chinese vehicles, unimaginable in Western markets a decade ago, are displacing incumbents across Europe, Latin America, and Southeast Asia.[296] Canada, America's largest trading partner, is considering Build Your Dreams (BYD) assembly plants on its own soil.[297] Chinese firms hold ownership stakes in roughly 10,000 U.S. auto-parts suppliers.[298] China's share of global manufacturing exports climbed from 5 percent in 2000 to 20 percent in 2023, while America's fell from 14 to 8 percent during that time.[299] Not even COVID-19, which should have been a wakeup call, stirred America to address its own dependencies.[300] Put succinctly by Craig Tindale, an investment manager, "A country that cannot make, refine, power, move, and repair the physical systems it depends on can be remote controlled by a country that can."[301]

The case for action is not only strategic. Manufacturing is among the most economically stimulative sectors in the U.S. economy: Every dollar of manufacturing output generates $2.69 in total economic activity, and every direct manufacturing job supports roughly five others, with every dollar of manufacturing wages generating $4.33 in total labor income.[302] Advanced manufacturing, robotics, and AI will widen those ratios as well as increase productivity. China's industrial productivity gains have tracked closely with its robotics adoption, which far exceeds that of America's.[303] This makes growing the manufacturing base more important, not less, to sustain high employment and GDP.[304]

The U.S. government has already made a few moves to address the challenge, including the One Big Beautiful Bill of 2025, the Office of Strategic Capital's $200 billion authority, and the rare-earth and Pax Silica initiatives.[305] While necessary to boost the defense industrial base, these actions do not reach the broader commercial and industrial base or the "missing middle": the hundreds of thousands of manufacturers and dual-use suppliers that are the heart of America's production base.[306]

Here, I endeavor to make the case for revitalizing American manufacturing by explaining why economic statecraft fails without commercial manufacturing competitiveness; how, unlike software and services, manufacturing delivers low profitability, is starved for capital, and offers thin entrepreneurial rewards; which free-market levers could make America more competitive; and finally, what Congress should do, and when. It took 30 years for the United States to lose manufacturing. Rebuilding it will not be fast, easy, or free.[307]

Economic Statecraft Requires Near-Competitive Products

Economic statecraft involves offering superior products to allies at near-competitive prices, setting technical standards, building supply chain dependencies that create leverage, and threatening to withhold what you can provide credibly.

As the United States outsourced manufacturing in recent decades, it benefited from importing deflation.[308] Yet, at the same time, it lost foundational capabilities in shipbuilding, rare-earths processing, and producing pharmaceuticals, semiconductors, drones, robots, and batteries, among other products.[309] This has put a significant drain on GDP. Meanwhile, according to the Rhodium Group, an independent research firm:

> China's industrial policy is becoming more systemic and pervasive, extending across all layers of production from upstream inputs and industrial equipment to downstream applications, services, and frontier technologies ... Beijing also increasingly deploys policy tools to entrench its dominant position in global value chains and counter foreign diversification strategies.[310]

With 330 million people, versus China's 1.4 billion, the United States acting alone loses on scale. Instead, it needs the collective volume of its traditional allies and partners. With a total population of 2.7 billion and combined GDP of $34 trillion, Europe, Japan, South Korea, India, Australia, and much of Southeast Asia have the capital, technology, and market depth to compete with China. The math works, but only if American manufacturing can deliver on feature, function, scale, and price. Pivoting from a blunt tariff-centric approach to a tariff- and coalition-building one may be the glaring opportunity that U.S. leaders can soon (re)embrace.

Under the second Trump administration, a renewed strategic focus on the Western hemisphere shows progress with receding Chinese influence in Central and South America, including Panama, Peru, and Chile.[311] However, as the United States reasserts itself, trade is needed to back it up.[312] Over the last 25 years, Chinese trade in the region has grown from virtually nothing to half a trillion dollars a year.[313] Already by 2015, Beijing was the top trading partner for most of South America.[314] Since then, it has become an even more significant economic player.[315] Chinese exports of consumer goods, high-end electronics, and cars undercut U.S.-made products, while its outsized demand for commodities has drawn the region further into its orbit. Recapturing these markets requires competitive products.

Wealthy and Impotent

America is caught in a trap. Despite an immense debt load, the U.S. economy remains the envy of the world: GDP growth leads the G7 and unemployment is near historic lows.[316] The world's deepest capital markets, the world's reserve currency, and, historically, the strongest alliance network in history, undergird America's military and deficit spending.[317] Unresolved is the balance of cost and benefits accruing to the reserve currency holder.[318] However that argument resolves, a competitive manufacturing base is required to practice economic statecraft effectively.[319] For example, the United States and Canada have long co-built automobiles.[320] As Canada — America's second-largest trading partner — considers building Chinese BYD car factories at home, the message is clear: China's manufacturing depth, rapid product cycles, and leading battery technology deliver inexpensive, feature-rich cars.[321] Were Canada to strongly embrace Chinese vehicles, its trading relationship with America could fracture.

Ford is responding and expects to deliver a Tesla-competitive car in mid-2027 at BYD-level manufacturing costs.[322] Ford's actions will roll through its supplier base, spurring upstream reshoring, reinvestment, and revival. Such investments should be replicated widely.

Capital without manufacturing becomes financial extraction, not strategic investment. S&P 500 companies returned over $12 trillion to buybacks and dividends between 2015 and 2024 — capital that did not build factories.[323] Innovation without production becomes a gift to competitors. The United States invents while China manufactures.[324] Yet, America's import dependence — offshoring manufacturing on the promise of higher profits via lower manufacturing costs in China — gave Beijing the opportunity to scale as it innovated, copied, or stole capabilities.

Leveraging America's Strengths

America's institutional advantages are as real as its capital advantages. The United States combines an unusually high tolerance for entrepreneurial failure, a globally dominant startup ecosystem, deep public-private research capacity, and a venture-capital-centered financial architecture that rapidly flows capital to new ideas.[325] However, without competitive manufacturing, capabilities, skills, and capacity atrophy.[326] A country, or Congress, unable to finance manufacturing companies through the so-called valley of death from prototype to scale production or rebuilding capacity with software-led advanced capabilities donates its intellectual capital.[327]

Rebuilding the missing middle would strengthen every dimension of U.S. economic statecraft, deepening the production base that makes leverage real, reducing the import dependencies that adversaries exploit, and restoring the manufacturing credibility that makes the allied coalition offer credible.[328]

The choice America faces is either rebuilding critical domestic manufacturing or continued dependence on China. Currently, 70,000 American manufacturing companies import from 45,000 Chinese suppliers (notably, the 45,000 companies themselves buy from other Chinese manufacturers).[329] Rebuilding imputes a necessary choice: manufacturing output with automation-augmented jobs, a Rubicon China crossed years ago.[330] As a result, Chinese workers produce considerably more physical output per worker than do Americans — that lead compounds.[331]

Japan has eagerly adopted robots to improve productivity and offset a decline in its working population.[332] It has about 70 percent of the global market for robots.[333] In the 1980s, America adopted lean manufacturing, Japanese management, and production technologies.[334] Incentivized with capital and talent, America's entrepreneurs will be eager to learn from Japan and any other company or country.

One source of knowledge and experience will come from integrating defense manufacturing knowledge into commercial manufacturing, including in software, robotics, and AI augmentation. Defense firms including Hadrian, Anduril, and Divergent are leading the way, while Tesla is doing so in the non-defense sector.[335] Green shoots — in the form of software, AI, marketplaces, and robot companies — are beginning to appear.[336]

Robotics adoption should not be mandated or directed by government fiat. Instead, monetary incentives can help the free market rebuild domestic manufacturing.

A revitalized manufacturing sector with workers overseeing AI-optimized factory floors is how America leapfrogs its lost industrial base — and it's a big leap. The scope — likely hundreds of thousands of companies — is too large for government programs to pick winners.[337] The incentives should be free-market oriented and directed towards increasing domestic manufacturing value. Free-market means available to any manufacturing company, meeting some set of requirements, not going through a lengthy government application process, and not a function of personal or political connections.

What To Do

The free market is America's superpower. It's time to release it in three ways to rebuild domestic manufacturing. First, improving income statements through transferable tax credits scaled to the percentage of domestic value added which directly improves profitability.[338] Second, making credit more available via Mannie-Mac, bank-delivered low-cost manufacturing loans, funding expansion, investment, and improving profitability through a lower cost-of-capital.[339] Third, increasing rewards for entrepreneurs via a qualified small business stock-style exemption, designed for founders and leaders running and growing manufacturing firms, rewarding operators, not investors, for building manufacturing companies.[340]

IMPROVING INCOME STATEMENTS

It is no surprise that capital has fled manufacturing — it returns less money than other sectors. The result is a self-reinforcing cycle of low profitability, underinvestment, and capability attrition and outsourcing.[341]

New York University Professor Aswath Damodaran provides the most comprehensive public data and

analysis for corporate comparisons.[342] Against broad manufacturing in the United States, software, business services, and consumer services companies earn about 1.8 times the return on capital.[343] Against more narrowly focused capital-intensive sectors, the multiples are far starker, with software approximately 6 times more, services nearly 5.7 times more, and pharmaceuticals about 3.4 times more.

Transferable tax credits, scaled to the percentage of domestic value added, can deliver direct income statement support to established, middle market, and start-up companies as they invest in new facilities, equipment, products, people, and markets.[344] Improved profitability improves return on investment, attracting capital and talent.

INCREASING CAPITAL AVAILABILITY

Beyond profitability, the high cost of capital, when it is available, compounds the low return problem. U.S. small-to-midsize manufacturing firms borrow at 7 to 11 percent more than in China.[345] Small Business Administration loans, limited to five million dollars, charge 10 to 12 percent.

Independent of the cost of capital, the United States banking system does not finance domestic manufacturing at the scale or terms that a reshoring agenda requires.[346] The competitive disadvantage for U.S. manufacturers is a profitability, capital cost, and capital availability problem that tax policy alone (including the One Big Beautiful Bill) does not solve. Scaling production requires more money.

Mannie Mac, low-cost capital delivered by banks directly to companies, gets both the government out of winner-picking and companies out of multi-year application processes.[347] Like Fannie Mae and Freddie Mac, which drove home ownership, Mannie Mac can support mid-size companies in investing in advanced manufacturing to gain capacity, scale, and price.

REWARDING ENTREPRENEURS

Entrepreneurialism is another American superpower. Entrepreneurs and their employees take risks joining small companies, investing their time and sometimes capital in exchange for equity with the expectation of larger returns. However, since manufacturing companies generally return less money than software and services companies attracting talent to manufacturing requires the promise of additional returns.

The current applicable program, the qualified small business stock, rewards investors and employees with capital gains tax exemption, with strict $15 million limits per person or 10 times the share cost basis —whichever is greater.[348] However, the program applies only to C corporations, while many start-ups, family businesses, and existing manufacturing companies are S corporations or limited liability companies.[349]

The most direct free-market reward for entrepreneurs is money. Whether a founder buys an existing manufacturing business or starts a new one, increasing the monetary reward via a manufacturing-only capital gains tax exemption tilts the entrepreneurial calculus where it is needed. A significant capital gains exemption program, up to $250 million, across operational equity holders can support manufacturing company transitions from baby boomers to their children, and founders and management starting and running manufacturing companies.[350]

More than 100,000 manufacturing companies are expected to undergo ownership transition over the next decade as baby boomer founders retire.[351] Without intervention, these companies face private equity acquisition for asset extraction, sale to foreign buyers, and closure.

Talent follows capital, and capital follows returns.

Conclusion

Manufacturing competitiveness is the precondition for every other instrument of American power.

A country cannot practice economic statecraft effectively without competitive products to offer, withhold, and build upon. The military cannot defend the country without the industrial base to produce what defense requires at price and scale. The United States will not lead the technological future without the physical infrastructure to manufacture it, and America cannot make the allied coalition math work without a credible economic offer that closes the gap.

Solving for manufacturing means solving for relative profitability and returns, supplying low-cost capital for scale, innovation, and reshoring, and rewarding entrepreneurs for founding and running manufacturing companies. This takes U.S. government leadership and action. It will not happen by itself.

America is wealthy in the assets that matter — capital, talent, alliances, and innovation — and increasingly unable to deploy them because those assets lack physical expression. With every quarter that the manufacturing base continues to hollow out, the gap between America's potential and its deployable statecraft capacity widens.

America's superpower remains the free market, which responds to incentives. If America wants a different outcome, incentives should be changed — it cannot "winner-pick" its way to success. Government policy should not pick winners and must address upstream and downstream supply chains. Targeted industrial policy risks stranding isolated capacity, and current efforts on rare earths and semiconductors carry this risk. China has been building deep supply chains, while America has been losing them.

The investment required to compete is a fraction of the cost of the alternative — an America that cannot produce what its statecraft requires.

Mark Rosenblatt runs Rationalwave Capital Partners, an early-stage venture fund. He has analyzed, founded, ran, sold, and invested in technology companies for 45 years.

Manufacturing competitiveness is the precondition for every other instrument of American power.

CHAPTER 9 EPILOGUE: FROM MANUFACTURING RISK TO MARKET RENEWAL

Mark Rosenblatt

The current state of the U.S. manufacturing base presents both a risk and an opportunity. It's an opportunity because America's loss of critical capabilities, skills, and companies able to make things represents a chance to invest in new-style manufacturing, including AI, software, and robots, that can support more flexible production at lower cost without displacing recent, less capable capital investments that were never made. It's a risk because executing on this opportunity is difficult; China controls many of the required inputs and delivers world-class products across most sectors.

America's current manufacturing companies lack capital and are less profitable than other sectors, leading to both underinvestment and difficulty attracting talent. And the need to eliminate the Pentagon's critical dependencies on China has forced it and the administration to take urgent action across multiple sectors, including rare earths and semiconductors. This exigent sector-level industrial policy risks expanding into more and more sectors under the rubric of "national security," chancing the rise of government winner-picking that competes with the free market — the real U.S. "superpower." Finding the bridge between sector-level industrial policy and free-market manufacturing incentives is critical to closing our manufacturing risk.

If America cannot close the gap between Pentagon and administration actions and the free-market industrial ecosystem, its productive capacity will not be world-competitive in terms of features, scale, or price. Defense requirements do not require the scale of the commercial/industrial market, although they can and should ride on top of those markets' scale, technology, and price.

As the electric stack, new drugs and treatments, advanced materials, and AI-embodied physical products pervade the economy, America needs to lead in scale, features, and price to meet its own requirements and those of its trading partners.

These products all depend on deep supply chains from dirt to elements, materials, chemicals, components, and all the way up to AI. Dependency along the supply chain creates chokepoints. Delivery at the top creates leadership, economic value, jobs, increased Gross Domestic Product, and an improved standard of living.

The Flintstones' Bedrock City and the Jetsons' Orbit City illustrate the difference between manufacturing leadership and its absence. Is it any wonder that Germany and Spain are leaning toward Huawei? Canada is importing Chinese cars. FCC limitations on newly imported drone models, imposed late last year, lock out competition from evolving Chinese features and functions. America lacks a commercial drone supply chain capable of competing. China's manufacturing trade has blossomed as America's has stagnated, delivering Orbit City-level products compared with America's Flintstones.

America needs to decide where it wants to live, and soon.

Mark Rosenblatt runs Rationalwave Capital Partners, an early-stage venture fund. He has analyzed, founded, run, sold, and invested in technology companies for 45 years.

Editors' Note: This article was not accompanied by a webinar.

Finding the bridge between sector-level industrial policy and free-market manufacturing incentives is critical to closing our manufacturing risk.


sting Plant
Ford

CHAPTER 10

ABSTRACT

Economic security sits at the crossroads of business, security studies, finance, international trade, and technology, and few professionals can move fluently across all of them. Furthermore, there is not an established academic discipline focused on contemporary statecraft to produce professionals, in part because of misaligned incentives in academia; without an established field there is no tenure, funding, or status to earn. Cybersecurity and biotechnology traveled similar paths, each initiated by an emergent risk that led to an established profession. Economic security must now follow.

The article closes with three recommendations: reward interdisciplinary teams across the public and private sectors, to include integrating economic security in professional military education; build economic security into university curricula, starting with cross-department courses and growing into full degrees and certificates; and tie scholars to practitioners through joint appointments, funded sabbaticals, and sponsored research.

Scan the QR code to view the webinar that accompanies Chapter 10.

ACADEMIA'S CRITICAL ROLE IN DEVELOPING AN ECONOMIC SECURITY WORKFORCE

Jennifer Buss

The United States is fighting a new kind of global competition — over supply chains, chips, and sanctions. It barely has anyone trained to fight it.

No single country can untangle itself from the forces of global trade, and no industry can stabilize in isolation. Because of this dynamic, countries are increasingly leveraging and protecting their economies in pursuit of broader national objectives. This interconnectedness of global markets demands public and private sector professionals capable of thinking critically about economic security.

In the United States, the workforce and the pipeline to feed it does not yet exist at the scale the moment requires. Supply simply does not meet demand, and many of the practitioners dealing with economic threats have limited requisite formal education and training. Instead, they should be enterprising, working within organizational limits — and often on the periphery — with minimal or no resources, often in the absence of guiding strategies or doctrine. Compounding the challenge, economic security lacks an established professional track or workforce pipeline. Few people have the bona fides to move fluently across economics, security, finance, and technology. To remain a global leader, the United States should establish and maintain an economic security workforce, including by creating a new academic discipline, before the talent deficit hardens into a strategic liability.

Emergent fields like cybersecurity and biotechnology have developed into professions in recent years, but academia has been slow to adopt a path for economic statecraft as a discipline to follow suit. Success of that path will require rewarding interdisciplinary teams across the public and private sectors, embedding economic security in university curricula, and bringing scholars and practitioners into closer collaboration.

The Challenge: Economic Security as a Discipline

Economic security sits at the crossroads of economics, foreign affairs, security studies, finance, business, political science, and information science, among other subjects. This interdisciplinary nature makes economic security difficult to categorize and champion, complicating efforts to develop a workforce capable of thoughtfully addressing the myriad opportunities and challenges relating to economic statecraft.[352]

Academia builds a future workforce using structure and discipline — an adherence to certain guiding concepts, principles, and paradigms — and then fosters and reinforces this through formal education and professional development. Existing academic disciplines tend to be largely siloed, and few universities offer integrated curricula designed to master a multidisciplinary field like economic security. A discipline carries its own body of theory, accepted methods, dedicated literature, and degree pathways. This scaffolding allows professors to teach, research, and professionalize a subject at scale.

Consider the following three seemingly unrelated sectors: supply chain, finance, and technology. Supply chain security is not simply the economic principles of supply and demand, rather

it encompasses technological dependencies, international trade regulations, and geopolitical risks associated with sourcing materials. It might also involve employing economic tools, like sanctions, to pursue national policy objectives. During the novel coronavirus pandemic, decision-makers had to rapidly assess vulnerabilities in global supply chains for medical equipment, which required expertise spanning economics, logistics, public health, and international relations.[353] The reality proved messier than the officials managing the response expected, as the public health experts who set policy were often unaware of broader challenges within the ecosystem.[354]

To protect the financial system, specifically banking infrastructure, policymakers should also consider the risks posed by cyberattacks. This requires knowledge of finance, information science, cybersecurity, and international law. In 2016, hackers used the Society for Worldwide Interbank Financial Telecommunication banking network to steal $81 million from Bangladesh's central bank account at the Federal Reserve Bank of New York, and attempted to move nearly $1 billion.[355] Untangling it required bank officials, incident responders, lawyers, and diplomats. The attack, later tied to North Korea, required the same cross-disciplinary response that economic security routinely demands.

Finally, policymakers should balance national security interests and technological innovation against economic growth. The U.S. Department of Commerce's October 2022 controls on advanced chips and chipmaking equipment bound for China, tightened and expanded over the following years, show how export policy in this area depends on the teamwork of engineers, economists, business analysts, and lawyers.[356]

While the notion of economic security stands to reason, it isn't explicitly taught in classrooms or in corporate on-the-job training. This leaves a knowledge gap and the ability to mitigate risk, highlighting the necessity of cross-disciplinary experience for both public and private sector leaders. Without preparation and exposure to the broader landscape, policymakers and business leaders make decisions in isolation, lacking the holistic perspective required to address complex economic security challenges.

Closing this gap is a shared responsibility. Business leaders and policymakers each bring distinct but complementary tools, and the work only succeeds when the public and private sectors treat it as a joint undertaking rather than a problem for someone else to solve.

We've Been Here Before

Economic security is not the first new discipline to arise from a changing global landscape. Whether geopolitically or technologically based, we've learned to teach new skills, identify new risks, and develop strategies and approaches to address related challenges.

As technology evolves, fields of study follow, expanding application to new sectors while also extending risk to larger subsets of the population. Consider three recent case studies where new disciplines emerged: cybersecurity, biotechnology, and semiconductors.

CYBERSECURITY

As cyber threats became more sophisticated and widespread, impacting financial systems and critical infrastructure, the federal government pressed the academy to respond. In the early 2000s, universities generally treated cybersecurity as a specialization within broader information technology curricula.

By 2010, the National Security Agency and the Department of Homeland Security designated centers of academic excellence in cyber defense by establishing programs at dozens of universities including George Mason, Virginia Tech, and the University of Maryland.[357] Today, cybersecurity is not only taught under computer science programs, but also within law, business, and public policy degree programs. Degree tracks integrate technical training with policy analysis, ethics, and risk management, reflecting the needs of the executives and lawmakers who must navigate complex regulatory and security environments. This academic transformation has produced a new generation of cyber-ready professionals equipped

to address both technical and strategic challenges in the digital age.

BIOTECHNOLOGY

Similarly, advances in biotechnology spanning genetic engineering, pharmaceuticals, and bioinformatics have reshaped academic programs. The Human Genome Project, completed in 2003, helped turn a niche intersection of biology and chemistry into an array of academic disciplines.[358] Universities across the world formed specialized degrees and certificates in biotechnology, bioethics, and biomedical engineering, as a response to the availability of genomic sequencing and editing. As policymakers grappled with issues such as genetic privacy, bioterrorism, and global health security, academic curricula evolved to include regulatory science, ethical frameworks, and international policy. These courses expose graduates to the broader implications of biotechnological innovation, further preparing them for the workforce. While employees in the biotech industry are often highly specialized in their technical field, however, they are not regularly exposed to higher-order, more abstract implications of their work — to include aspects of economic security — which can put a company at risk.

SEMICONDUCTORS

The evolution of the semiconductor industry reveals how complex policy problems reshape academic programs. Semiconductors sit at the heart of technological innovation, powering everything from smartphones to fighter planes. However, their manufacture and regulation involve intersections of electrical engineering, materials science, international trade, economics, intellectual property law, and national security studies. Careers in semiconductors start with an electrical engineering degree, then require knowledge of scaling, supply chain, and business. The recent global chip shortages and the U.S. government's efforts to control the export of advanced semiconductor technology for AI further emphasizes the need for an interdisciplinary approach to both research and policy, incorporating an understanding of geopolitics and geoeconomics.[359] The Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act of 2022, which paired tens of billions of dollars in manufacturing incentives with money for workforce development, incentivized universities to stand up semiconductor programs and research centers that expose engineering majors to business, policy, and international affairs.[360]

While these examples highlight technical developments, policy and workforce issues may arise in any emerging discipline. For the United States, the practical consequence is a shortfall in economic security expertise and practice — a strategic gap that demands deliberate remedy.

Professional Dialogue

The above examples demonstrate how emerging risks and policy challenges drive academic evolution, as well as how the resulting disciplines arose from societal needs, not organically from academia. In each case, grassroots campaigns emerged, recognizing a gap in professional societies' or existing communities' offerings in both the public and private sectors. Like-minded professionals sought each other out and created forums for problem solving and debate.

As the conversation evolves and more people join the dialogue, existing conferences begin adding panel discussions on the emerging topic. Further expansion of the community produces entire conferences dedicated to the developing topic. The end of this spectrum is just as instructive. The continuing-education regimes that govern accountants, attorneys, and physicians — required coursework, credentialing, and recertification — are part of what define those callings as professions and hold practitioners to a shared standard discipline throughout their career.

Through these interactions, passionate individuals build a shared framework bridging theory and practice. They then take this communal thought into their workplace, making decisions with their newfound broader experience. Sound decision-making relies on professionals educated in or experienced in many (or all) of the disciplines mentioned above. Strengthening experience in an emerging field such as economic security rests, for now, on the small number of people already working in the field. Ad hoc organization is not an enduring model for a discipline so vitally important to U.S. security and prosperity, which is why widening exposure and expertise across government and industry is so urgent.

Creating an Academic Discipline

By adapting degree programs to meet new demands, universities can deliver the cross-disciplinary expertise necessary to address evolving threats and establish a pipeline of professionals focused on economic security. University deans do not make light of offering new degree programs — it's a business decision at its core. So, what is the business case for investing in economic security as an academic discipline?

Academic programs require a curriculum and a theoretical framework driven by professors, graduate students, and academic researchers. Practitioners also play a vital role, especially as catalysts, leveraged as adjunct teachers drawing on real-world experience. Many universities rely on adjuncts — part-time professors who work in the profession — to ground academic theory in practice. This is an important part of a holistic approach to developing curricula for economic security.

Individual courses and integrated degree programs in economic security have emerged at a handful of institutions, including Johns Hopkins University, Georgetown University, George Washington University, and Texas A&M University. Of those four, only the Bush School of Government and Public Service at Texas A&M has a dedicated economic statecraft program.[361] The others teach economic statecraft within existing security and economics degrees, as with Johns Hopkins' School of Advanced International Studies, alongside its required international-economics core.[362] Adjuncts at these schools are often former government officials, industry practitioners, or risk managers.

Scholars and practitioners are now debating the vernacular and scope of economic security.[363] In existing courses, professors have started to include topics such as supply chain resilience, technological dominance, resource security, industrial policy, export controls, tariffs and trade restrictions, investment diligence, and the protection of infrastructure. Continued dialogue will help establish standards, smooth barriers between academic fields, and integrate lessons from the field into curricula.

The Incentive Hurdle

Creating a new academic discipline is disruptive. Academic incentives are currently misaligned against economic security, and that misalignment is largely why the field does not evolve, as the people best positioned to build it have every professional reason not to invest their time.

Traditionally, academics are incentivized by publishing papers with the goal of advancing knowledge and inviting others to build on their ideas — they are driven by reputation and scholarship, measuring their worth by their contributions to the subject matter and how far their ideas have spread. This impact requires sufficient funding from grants or donors to support a professor's research and publish their results.

Academics also respond to earning tenure, citations, and status in a recognized field. Economic security offers none of this yet, because it is not an established discipline.

Meanwhile, revenue drives universities, operating as businesses within a competitive global landscape.

Universities attract the best talent, the most recognized experts in the field, with a strong compensation package often including modern offices and lab space, dedicated staff, and a competitive salary. They expect significant revenue, from donor contributions and/or federal grants, to the university based on the addition of new scholarship.

Here's the catch: These incentives only align when a field of study is well defined. Expanding existing fields to include economic statecraft will be the first milestone to disrupt the siloed academic rigor required for publication. The more ambitious alternative is to stand up a wholly new integrated field built for this reality, one designed from scratch to produce the talent and leadership the United States needs to stay competitive in the world.

Recommendations for Building a Robust Economic Security Workforce

Three main recommendations arise to develop future economic security professionals.

First, reward interdisciplinary teams across the public and private sectors. Agencies and firms should require fluency across disciplines. It should be written into how they hire, promote, and award contracts, so that pairing technical and policy expertise becomes the norm rather than the exception. Business teams should include members with MBAs, Ph.D.s in technical fields, and social science degrees, to span the economic security ecosystem. The same logic applies in uniform. Combatant commanders and service chiefs should build economic security into planning the way they already account for logistics and intelligence. That means assessing how sanctions, supply chain exposure, and an adversary's economic leverage bear on an operation, and staffing teams with people who can run that analysis. Professional military education should build the know-how to operate at the intersection of security and economics. This is why institutions like the National Defense University's Eisenhower School for National Security and Resource Strategy — which aims to help government leaders better understand industry — have started including economic security issues in coursework, so commanders, planners, and strategists can weigh it in their decision-making.

Second, universities should incorporate economic security into academic programs. They should start with courses shared across departments and joint research that bridges economics, security studies, political science, business, and information science, then grow those into full graduate degrees in economic security and certificate programs that keep working professionals current. In the interim, public and private institutions should invest in focused professional development so the workforce can evolve to what universities will eventually produce, while also meeting urgent needs.

Third, incentivize collaboration between scholars and practitioners. Joint appointments, sabbaticals funded by the host agency or firm that let faculty and practitioners move between the campus and the field, and sponsored research from both government agencies and industry will help keep theory tied to practice. Corporate investments in university partnerships, associations, and conferences are also some of the most valuable paths to promoting dialogue and collaboration, a requirement for an effective societal-level approach to economic security.

A workforce adept in addressing complex public and private sector economic security challenges is a strategic necessity for the United States. Preparing the next generation of economic security-minded professionals requires a fundamental shift in academia and society. China has spent years cultivating talent and influence in U.S. universities, a phenomenon the House of Representatives' Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party documented in a recent report.[364] Economic security is gaining traction as a stand-alone discipline — an initial foundation for a community of academics and professionals across government and industry who share a common language. Degree programs, certificates, and continuing education to mature the field should sustain this community.

By investing in interdisciplinary education, fostering collaboration, and shifting incentives, the United States can build a workforce equipped to master the evolving landscape of economic statecraft, ensuring American interests remain secure in an increasingly interconnected world.

Jennifer Buss, Ph.D., is the Chairman and CEO of the Potomac Institute for Policy Studies. The Institute works with thought leaders to anticipate and address science and technology issues facing our society. She advises senior leaders in the public and private sectors and currently serves on the advisory boards of defense firms and startups. She has a doctorate in biochemistry from the University of Maryland and is married with two children.

CHAPTER 10 EPILOGUE: THE CHANCE TO ADVANCE ECONOMIC STATECRAFT IN PROFESSIONAL MILITARY EDUCATION

Kimberly Sloan

The Professional Military Education (PME) system provides officers and senior enlisted service members with a fully funded curriculum focused on the skills, knowledge, and abilities needed to operate across the spectrum from competition to nation-on-nation warfare.[365] Economic statecraft applies across that spectrum, but PME institutions like Air University (AU), Army War College (USAWC), and National Defense University (NDU) do not currently offer accredited economic statecraft programs. The schools are open to curriculum changes; for example, Dr. Buss noted that NDU's Eisenhower School for National Security and Resource Strategy has begun incorporating lessons on economic security. Before proposing wholesale curriculum changes, readers should first understand the impact of suggested changes.

The Challenge of the Economic Statecraft Profession in PME

The military's education system is designed to develop students to meet military technical, managerial, or professional needs[366] — in essence, preparing officers and senior enlisted service members for their next job. NDU and AU are resourced to develop students for future operational and command assignments. However, there is no economic statesperson role in the military. Therein lies the problem. If you do not have the demand, supply is hard to build. Adjacent positions in defense do exist, for example, Foreign and Civil Affairs Officers, Defense Intelligence Analysts, and Acquisition and Financial Management, but their flavor and focus are more general than specialist. In this case, it is difficult to develop an academic program focused solely on training for a job that does not yet exist.

Opportunity to Advance Military Economic Statecraft Professionalism

27 February 2026 PME policy guidance from the Secretary of War emphasizes a renewed focus on "the preparation of senior officers to be critical thinkers that can plan and integrate multi-domain, Joint operations at echelon and serve (and think) at the strategic level."[367] Arguably, this charge could support expanding PME programs to include an economic dimension.

The military recognizes the need for economic statecraft, for example, the Office of the Secretary of Defense created the Office of Strategic Capital a few years ago, the Economic Defense Unit this year, and the Air Force is establishing an Office of Expanded Competition under the Office of the Secretary of the Air Force.[368] The 2026 National Defense and 2025 National Security Strategies[369] also emphasize the importance of economic security, but the challenge for professional military education remains twofold. First, the military must weigh the implied cost of supplying a funded economic statecraft program against job demand; second, it should provide specific guidance on creating a program that still adheres to the military values service members are sworn to uphold.

The PME Value of an Economic Statesperson

In the academic practice environment, the implications of economic statecraft on prosecuting military missions might best be exposed to military planners during the capstone course, which is designed to test what students learned, sometimes in simulated "real and live" events like a wargame. Commonly, wargame scenarios focus on military objectives

such as overcoming logistical supply chain barriers, marrying munitions and platforms to prosecute targets, and — more recently — conducting battle damage assessments following cyber activities. Over a decade of experience in national and service wargames taught me that if participants discussed economic impacts, it was largely an afterthought, debated among a small group while the rest of the team broke for lunch. More likely, it was during a separate tabletop event focused on the "D," "I," and "E"[370] aspects of national power, and junior and mid-tier military personnel did not participate.

Overcoming Challenges to Military Economic Statecraft Professionalism

Addressing the cost requires more than identifying budget space to establish a full PME program; it also requires identifying and leveraging currently available trained personnel, existing courses, and drafting special experience identifiers to track and determine how the Pentagon can best employ their knowledge.

While PME professionals are developing an accredited program for economic statecraft, an interim solution could be leveraging existing fellowship opportunities at civilian institutions. As noted by Dr. Kellogg in her article, "Operationalizing Economic Statecraft: A New Imperative for the Pentagon,"[371] the "craft" is primarily held in the private sector. In line with the Secretary of War Hegseth's memorandum, Senior Service College opportunities could include attendance at civilian institutions with economic statecraft programs and courses. Further, attendees could report their experiences and lessons learned from the program back to PME staff to help build their own curriculum.

Additional interim solutions include slightly modifying existing military course curricula, tests, tools, and wargames to include economic statecraft. The following is an initial list:

- Expanding the All-Domain Maneuver course at AU, which currently provides mission analysis across six domains — land, maritime, air, space, electromagnetic spectrum, and human,[372] to include an economic domain.
- Developing an economic statecraft objective in AU's International Officer School (IOS). This school prepares international students for Air War College, Air Command and Staff College, and Squadron Officer School through student immersion experiences. Over its 100-year history, the school has graduated more than 11,000 international military students, including future air chiefs, chiefs of staff, and heads of state from more than 140 countries.[373] The capstone event could include other AU students, which would spotlight economic statecraft's global nature and, as noted by a former Air Force Chief of Staff at a 2022 Global Air Chiefs Conference, the requirement for "internationally-minded" warfighters.[374]
- Leveraging tools that will be available throughout a service member's career during a real-world simulated capstone event to underscore the value of leveraging economic statecraft professionals to warfighters. GigEagle is a virtual tool that can rapidly identify and match available Department of War personnel, including Reserve and Guard components, with skills required for a crisis like COVID-19.[375] The military could use this tool during mission analysis and later to identify potential speakers or professors for courses.

Bottom line, creating a program does not mean starting from scratch. However, a one-off modification in a course here or there does no more than satisfy an awareness that global economic and military security are intertwined in warfare. An interim solution could help demonstrate that the demand for an economic statecraft professional workforce justifies the cost of funding a PME program.

Specific guidance on a PME program could emulate programs in civilian academia. While there are a few civilian institutions that address economic statecraft like Texas A&M, the University of Tennessee, MIT, and Stanford, Dartmouth has recently created a four-year pilot program that highlights economic statecraft through cross-disciplinary collaboration between its Department of Economics, Department of Government, Tuck School of Business, and John Sloan Dickey Center for International

Understanding.[376] What if the military were to replicate similar curricula but draw upon the expertise of Defense members? For example, having members of the Departments of Commerce, the Treasury, and State as guest speakers to align students' independent research, or as advisors during capstone events to provide active feedback on current problems and solution approaches.

While not an exhaustive list, a few other options to examine include:

- Sourcing strategic reserve forces, i.e., individuals with both economic statecraft and Defense expertise, to fill guest speaker, advisor, or professorial positions in the program. For example, the Air Force Reserve has cordoned off certain reservists with civilian expertise to leverage in a dual-use fashion.[377] They have a "bullpen" for hypersonic Ph.D.s, as well as China experts, and are exploring other areas.[378] The idea is that, instead of just capitalizing on their military education and training, the nation must also draw on their civilian expertise. This could provide a way to leverage individuals already trained in economic statecraft and security by civilian organizations, while preserving the craft for military outreach.

- Testing and adjusting the program's curriculum based on capstone feedback, where dual-use reservists advise future economic statecraft professionals, commanders, and planners on the implications of campaign activities during mission planning. This interaction sets the conditions to underscore the value of leveraging economic statecraft to warfighters. Demonstrating the curriculum's value for military operations, in turn, allows educators to advocate for funding to align curriculum to creative military power operations.

Recent events like the U.S. and Iranian military operations in the Strait of Hormuz and escalating fuel prices highlight the global interconnectedness between military power and the economy. What if that wargame from that AU class brought in an expert to discuss the impact of fuel prices on not just the air refueling plan during mission analysis, but also the forecasted impact and duration on the national or international economy? Education that focuses solely on military power misses opportunities offered by other parts of the DIME. Leveraging academia can help build an economic security workforce within the military, ensuring commanders are adequately equipped to plan for the economic domain's impact on the prosecution of military missions.

Kimberly Sloan, Ph.D., is the Director of Research Strategy and Development at the Potomac Institute for Policy Studies. Leveraging 20 years of active-duty experience in the U.S. Air Force, her research expertise focuses on intelligence, defense, concept development, targeting, and wargaming.

An interim solution could help demonstrate that the demand for an economic statecraft professional workforce justifies the cost of funding a PME program.



CHAPTER 11

ABSTRACT

Contributors to the *War by Other Ledgers* series mapped important facets and highlighted the challenges and opportunities of contemporary economic statecraft, both practiced and conceptual. In June of 2026, Treasury Secretary Scott Bessent outlined a strategy framework for economic statecraft. However, the doctrine, a guide for strategy implementation, has yet to be formally developed and adopted in concert with existing practices and guidance.

Ongoing efforts across the executive and legislative branches, industry, academia, and policy community are underway to employ U.S. economic statecraft. But success in implementing Bessent's strategy will require that doctrine be developed and orchestrated collaboratively across these communities, given the multifaceted and societal-level nature of the challenge.

Scan the QR code to view the webinar that accompanies Chapter 11.

WRITING THE PLAYBOOK: A STRATEGY AND DOCTRINE FOR AMERICAN ECONOMIC SECURITY

Tim Welter

In January, this article series opened with a blunt question: Economic statecraft is back, but is America ready?[379]

Driving the question, in part, was the fact that the United States had not yet articulated (at least overtly) a strategy for economic statecraft. This was despite widening recognition that nations were increasingly using economic tools like tariffs and sanctions to pursue strategic objectives.[380] U.S. awareness was particularly elevated by the realization during COVID-19 that decades of Chinese market manipulation, predatory trade behaviors, and security vulnerabilities deployed against its markets had gone unanswered.[381]

On the eve of the nation's 250th anniversary, Treasury Secretary Scott Bessent fired a shot across the bow. He announced a framework for economic statecraft driven by "the disciplined use of America's economic power in service of our sovereignty," embracing Alexander Hamilton's principle that every nation "ought to endeavor to possess within itself all the essentials of national supply." The strategy, which Bessent delivered to the Economic Club of New York and outlined publicly in the *Wall Street Journal*, centered on five principles: economic security begins with national capacity; American openness will be matched by reciprocity; America will write the rules of the next economy; financial leadership is a central instrument of statecraft; and economic statecraft should serve the American people.[382]

Bessent's five principles are generally an amalgamation of bipartisan economic statecraft concepts pursued since at least 2011 (albeit a departure from 80-plus years of post-war, Bretton Woods-framed geoeconomics).[383] They also underscore the difficulty of crafting a comprehensive economic strategy given very real tradeoffs between America's economic exceptionalism and its national security goals. Tensions among the strategy's principles are evident. For example, economic security derived from national capacity harkens to autarky, but American openness enabled by reciprocity points toward conditional engagement in an international trading system.

Despite its unproven state, Bessent and the executive branch have framed an overdue and much-needed strategy for economic statecraft. While the speech was a clarifying point for planners at Treasury, Commerce, the State Department, the Combatant Commands, and other agencies, the doctrine to follow — the guide for the strategy's implementation — is yet to be developed and should be adopted in concert with ongoing practices and guidance, while holding true to national values, institutional norms, and an independent private sector. That will require engagement with lawmakers, industry, and academics to reconcile tensions, and so practitioners are productively mobilized to realize the strategy's vision. While current efforts across the executive and legislative branches, industry, academia, and policy communities can serve as helpful guides, they are generally siloed and uncoordinated. Success therefore demands that doctrine be developed and orchestrated collaboratively across these communities.

Enabling elements include designating a "referee" for economic statecraft in the executive branch, a settled "home" for it in Congress, paradigm-shifting incentives for industry to partner with government, workforce investment, and evolution in academia. While many tradeoffs remain unresolved, these and future policy solutions will help leaders recognize and accept the risks required for meaningful change.

The Executive Branch

Bessent's speech is the most senior entry in a rapid buildup of economic security policy activities across the executive branch this year.

In April, the Pentagon's Deputy Secretary of Defense Stephen Feinberg formally established the Economic Defense Unit, a hub charged with fusing economic leverage and requirements into joint military planning and operations by developing requirements for economic competition activities.[384] It joins the Office of Strategic Capital in a growing Pentagon ecosystem focused on gaining strategic advantage via economic leverage.

The analytic foundation for that pursuit is also underway. The Defense Advanced Research Projects Agency's quantitative and rigorous theoretical footing.[385] A companion effort, the Anticipatory and Adaptive Anti-Money Laundering program, targets the machinery of illicit finance.[386] For a discipline that lacks objective metrics and testable models due to its nascency, wargaming geoeconomics with rigor and intentionality is a necessity to build confidence in practice, policy, and process.

The work ahead requires putting the strategy on paper so bureaucracies can consider and ingest it into process and practice. Bureaucrats thrive on regulatory guidance, as it is their impetus for action or inaction (and thus Congressional oversight). Bessent's five principles deserve similar treatment to what the National Defense Strategy does for the military instrument: a published economic security strategy nested within the national security strategy, with interagency doctrine and campaign plans following in turn.

Ongoing doctrinal work is ripe for adoption and then operationalization but it should be synchronized. The core task requires integrating economic considerations into both joint planning and the combatant commands, where commanders hold the day-to-day partner relationships upon which multilateral pressure campaigns depend.[387] Success will require building requisite playbooks and wargames to give Washington options when a crisis arrives. To execute, the executive branch should establish an entity akin to the Economic Warfare Operations Capability with definitive authority to prioritize and act on offensive and defensive economic statecraft decisions.[388] It should be informed by a joint public-private fused intelligence and analytics enterprise, in conjunction with domestic and foreign industry partners.

Congress

Congress is engaged, having recently pursued or passed various legislative initiatives, reports, and appropriations related to economic statecraft, to include the 2024 codification of the Office of Expanded Competition.[389] In contrast, Congress did not include language authorizing the Economic Defense Unit in the Fiscal Year 2026 National Defense Authorization Act, despite notable bipartisan support.[390] Passage this year is similarly uncertain, though the unit is still authorized to operate by Pentagon memo with $500 million in Congressional funding.

Legislative branch oversight fora like the Congressional-Executive Commission on China, the U.S.-China Economic and Security Review Commission, the House and Senate intelligence committees, and those overseeing commerce and foreign affairs, actively deliver proposals and recommendations on economic statecraft issues.[391] The House Select Committee on the Chinese Communist Party has especially proven itself as an active bipartisan forum focused on advancing U.S. economic competitive advantage.[392]

Yet challenges remain as economic statecraft lacks a single defined path for legislation and oversight on the Hill.[393] While the House Select Committee's charter sanctions investigative authority, it does not grant legislative jurisdiction.[394] Instead, its members work through other committees to advance legislation into law — not ideal given the magnitude and scope of the challenge and the competition for time and attention on busy legislative agendas.[395]

All these activities under Congress's charter — oversight, sunset clauses, reporting requirements, review and validation of policies, statutory latitude and guardrails on new authorities — grow trust in emerging doctrine, which, in turn, helps turn strategy into practice.

The codification of entities like the Office of Expanded Competition or the Economic Defense Unit by Congress elevate and establish inter-agency economic statecraft authorities that endure beyond administrations.[396] More broadly, it helps establish a dedicated home for economic statecraft, whether via a dedicated committee or a coordinating body among House and Senate committees that oversee jurisdiction of economic security-related issues.

A settled home in Congress, whether via a dedicated committee or a coordinating body among House and Senate committees that oversee jurisdiction of economic security-related issues, would give Bessent's strategy a durable legislative branch counterpart.

Industry

Over the last decade, industry has been forced to reconcile, often reluctantly, with its frontline role in contemporary economic statecraft.

Why the tension? Economic and political decisions once limited to local or regional impact now reverberate globally at unprecedented speed and scale. Once mundane corporate maneuvering from routine purchases to major mergers and acquisitions, capital investments, and manufacturing decisions, now translate to strategic leverage.[397] The ability of the United States to apply economic pressure ultimately rests on the combination of individual chokepoints and production, finance, supply capacity, and capabilities wielded by corporate America.

A strong enduring U.S. strategic posture will require continued overhaul of how public and private sector actors collaborate domestically and abroad.[398] Fusion of government and business intelligence is an enabling vehicle, required to inform board-level decision-making with statecraft implications while establishing doctrinal bona fides in both domains.[399]

Legal and ethics codes, like elements of the Federal Acquisition Regulation that define the statutory bounds of government and business interactions, should be reviewed and adjusted to ensure threats are meaningfully addressed jointly (and incentivized accordingly), while holding true to long-held societal values and free market norms.[400]

Industry should expect clear signals of policy and intent from the government as boards and executive teams renew their approach to due diligence, especially those with significant exposure or involvement in markets inherently vital to national security.[401] An open channel for continuous public-private dialogue, a clearinghouse to jointly mitigate or resolve unintended missteps, is in order to facilitate.

Private-public efforts like J.P. Morgan's Security and Resilience Initiative, non-profit organizations like Business Executives for National Security, the Pentagon's Business Operators for National Defense program, and purposeful guidance of capital toward national security-relevant sectors demonstrate progress on shifting culture and practice.[402] But evolution with staying power in both domains is still required for enduring economic security.

While policymakers are expected to lead, industry is firmly in the driver's seat. Much like the storied journey that led to an effective public-private approach to cyber security, the two sectors should come together to develop and deploy a doctrine to implement the nation's strategy for economic statecraft.[403]

Academia and Workforce

Just as economic statecraft lacks a home across government, the discipline lacks a settled home in academia, caught somewhere between economics, political science, security studies, and business. A ready workforce capable of navigating contemporary economic statecraft will require more intentional engagement and investment.

The tide is shifting. Institutions like the Eisenhower School for National Security and Resource Strategy have long filled a gap in helping military leaders understand and plan for the impact of adversarial economic statecraft on the ability to execute military missions.[404] Civilian programs like Texas A&M's Economic Statecraft Program at the Bush School

of Government are furthering intellectual rigor and academic programs.[405] And the Defense Advanced Research Projects Agency's National Security Economic Theory program will contribute to both realms, civilian and military, in its pursuit to define a more rigorous scholarly field for contemporary quantitative geoeconomics.

Academics should embrace interdisciplinary education, collaboration, and shifting incentives to drive scale and structure.[406] Universities can begin by formalizing curricula and credentials that prepare graduates for government and industry alike. The skills needed to staff a Treasury sanctions team will doubtless be transferable to corporate policy intelligence shops.

The workforce pipeline is its own front in the global competitive environment, with an incredibly long lead time. Every element of Bessent's strategy, from enforcement to analysis to campaign planning, will require people educated and trained to carry it out.

The Policy Community

The defense policy community has advanced doctrinal approaches and proposed frameworks for economic statecraft. As with the other communities, their work should be digested and analyzed by public and private sector leaders for integration into ongoing operations and contingency planning.

Two major works appeared this spring. *Emily Kilcrease's Hit It with Your Best Shot: An American Doctrine of Economic Pressure* distills 20 historical cases of American economic pressure into nine doctrinal principles, anchored by three theories campaigns should articulate in advance: a theory of victory, a theory of failure, and a theory of restraint.[407] Elaine Dezenski and Josh Birenbaum's Gameplan for American Economic Security proposes principles the United States should defend with its economic power and an "Economic Pentagon" to coordinate the effort.[408] Likewise, the Potomac Institute's 2025 Economic Statecraft Summit Report recommended a federal convening authority, an analytic enterprise, and oversight mechanisms to enable elements proposed in previous sections of this article.[409]

Bessent's June remarks now sit alongside these proposals, among others.[410] Despite differences, there is overlap between mutual ideas of centralized orchestration, anticipatory planning, and disciplined practice as necessary doctrinal tenets. The yet-to-be-named entity should next translate that convergence into references and tools for practitioners' use — operational handbooks, metrics of success, and wargame designs — for the interagency to exercise with and learn from alongside private sector partners.

Conclusion

U.S. adversaries and friends are carrying out their own economic statecraft strategies. China in particular is well-versed at waging economic war through supply chain coercion, intellectual property theft, cyber attacks, boardroom chess, and manufacturing base mastery.[411] Its successes means the U.S. government and its public and private sector partners, at home and abroad, must act quickly.

The "War by Other Ledgers" series elevated what should be acted upon, both in practice and concept. Across the federal institutional architecture, authorities and decision-makers remain decentralized.[412] Fused intelligence will close seams across public and private sector actors and better focus improvised operations by the Pentagon and other federal entities in the absence of a strategy and clear doctrinal framework.[413] Corporate leaders are learning to assess risk given new geoeconomic realities while grappling with how to grow and develop a workforce for today and tomorrow.[414] All point to the same condition: Siloes of excellence across the government and private sector are working ad hoc and disparately on economic security and will benefit from the connective tissue of a holistic national strategy and doctrine for economic statecraft.

Wholesale agreement on any administration's approach to policy is perpetually elusive. Bessent's strategy to economic statecraft strategy is no exception and will need to overcome critics of its principles and practice. Regardless, there is undeniable momentum for change across the stakeholder communities that should be translated into action.

Bessent's strategy offers an outline for a playbook yet to be drafted. The ledgers are open. Will the United States do what is necessary to balance them?

Tim Welter, Ph.D., is a senior research fellow at the Potomac Institute for Policy Studies, where he started and leads the Global Competition Project. Leveraging experience from Capitol Hill, the Pentagon, industry, and academia, his research is primarily focused on national security policy development and implementation, and economic statecraft.

The views expressed in this article reflects the author's personal thoughts and do not represent the position of the Department of the Air Force or the Department of Defense, with whom the author is also affiliated.

Siloes of excellence across the government and private sector are working ad hoc and disparately on economic security and will benefit from the connective tissue of a holistic national strategy and doctrine for economic statecraft.

ENDNOTES

	$96,325,000
	$748,900,000
	$4,283,750,000
	$327,600,000
	$1,094,250,000
	$58,875,000
	$6,742,300,000
	$413,825,000
	$2,875,600,000
	$127,450,000
	$935,275,000
	$8,164,900,000
	$274,625,000
	$144,560,000
	€247,670,000
	€3,042,800,000
	€219,650,000
	€11,425,700,000
	€546,825,000
	€1,287,400,000
	€5,200,000,000
	¥1,675,000,000
	¥7,125,000,000
	¥2,925,000,000

Introduction

1 Megara. (n.d.). In *Britannica*. Retrieved May 14, 2026, from https://www.britannica.com/place/Megara-Greece; The Megaran Decree. (n.d.). *CIRIS*. Retrieved May 14, 2026, from https://www.ciris.info/learningcenter/the-megaran-decree/.

2 Morley, N. (2010). 'The Emporium of the World': The Economic Impact of Empire The Economic Impact of Empire. In *The Roman Empire: Roots of Imperialism* (1st ed., pp. 70–101). Pluto Press. https://doi.org/10.2307/j.ctt183pb5x.8.

3 Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351.

4 *Economy & Trade*. (n.d.). United States Trade Representative. Retrieved May 14, 2026, from https://ustr.gov/issue-areas/economy-trade.

5 Siripurapu, A., & Berman, N. (2023, July 19). *The Dollar: The World's Reserve Currency*. Council on Foreign Relations. https://www.cfr.org/backgrounders/dollar-worlds-reserve-currency.

6 Bernanke, B. S. (n.d.). The dollar's international role: An "exorbitant privilege"? *Brookings*. Retrieved May 14, 2026, from https://www.brookings.edu/articles/the-dollars-international-role-an-exorbitant-privilege-2/; Harithas, B., Meng, K., Brown, E., & Mouradian, C. (2025). "Liberation Day" Tariffs Explained. *CSIS*. https://www.csis.org/analysis/liberation-day-tariffs-explained.

7 Lutnick, H. (2026, January 20). Why the Trump administration is going to Davos. *Financial Times*. https://www.ft.com/content/a675b8af-46b7-4f93-a616-41f0a002c22e.

8 *Analysis: China's Economy and Its Influence on Global Markets*. (2025, February 20). US Bank. https://www.usbank.com/investing/financial-perspectives/market-news/chinas-economic-influence.html; Mardell, J. (2017, October 25). The 'Community of Common Destiny' in Xi Jinping's New Era. *The Diplomat*. https://thediplomat.com/2017/10/the-community-of-common-destiny-in-xi-jinpings-new-era/.

9 Ip, G. (2025, December 6). China's Growth Is Coming at the Rest of the World's Expense. *The Wall Street Journal*. https://www.wsj.com/economy/trade/chinas-growth-is-coming-at-the-rest-of-the-worlds-expense-99420396?gaa_at=eafs&gaa_n=AWEtsqdafGeJD92RM1_SwsGJi0H0pEC4qtgn8CkasAw1GWjCgvAaMlUGdwhd_RcNZUI%3D&gaa_ts=693ee114&gaa_sig=M8n-f4PQMiAoNKuviykzn4m0arfNVPMEcvZ89-5KZdwgkf6HZ0ip3ddHXwZVCUaBDnj3We8kSGou-dNv8CtBkA%3D%3D.

10 Allison, G., Kiersznowski, N., & Fitzek, C. (2022). *The Great Economic Rivalry: China vs the U.S.* The Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/great-economic-rivalry-china-vs-us; *Remarks by the President at the U.S./China Strategic and Economic Dialogue*. (2009, July 27). The White House. https://obamawhitehouse.archives.gov/the-press-office/remarks-president-uschina-strategic-and-economic-dialogue.

11 Tatsumi, Y., Rawlins, M., & Siebens, J. (2025). *Economic Coercion from the People's Republic of China*. Stimson Center. https://www.stimson.org/2025/economic-coercion-from-the-peoples-republic-of-china/.

12 Wright, R., & Lu Stout, K. (2025, June 16). Shipping chaos: Inside the industry at the frontlines of the US-China trade war. *CNN*. https://www.cnn.com/2025/06/16/business/us-china-trade-war-shipping-industry-intl-hnk.

13 Chafetz, G. (2023, July 31). How China's Political System Discourages Innovation and Encourages IP Theft. *The SAIS Review of International Affairs*. https://saisreview.sais.jhu.edu/how-chinas-political-system-discourages-innovation-and-encourages-ip-theft/; Kim, T.-Y., Dhir, S., Dasgupta, A., & Scanziani, A. (2025, October 23). *With new export controls on critical minerals, supply concentration risks become reality — Analysis*. IEA. https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality; Scanlon, R. (2024, December 19). *How China's Antitrust Tactics Undermine U.S. Tech Leadership*. CNAS. https://www.cnas.org/publications/commentary/how-chinas-antitrust-tactics-undermine-u-s-tech-leadership; Stevenson, A. (2025, November 18). We Now Have a Better Picture of China's Global Lending Spree. *The New York Times*. https://www.nytimes.com/2025/11/18/business/china-loans-financing.html; Yong, N. (2023, January 16). Industrial espionage: How China sneaks out America's technology secrets. *BBC*. https://www.bbc.com/news/world-asia-china-64206950.

14 Baskaran, G. (2026). New Executive Order Ties U.S. Critical Minerals Security to Global Partnerships. *CSIS*. https://www.csis.org/analysis/new-executive-order-ties-us-critical-minerals-security-global-partnerships; Brennan, D. (2026, January 18). Europe "united" in face of Trump's Greenland threats, tariffs, EU chief says. *ABC News*. https://abcnews.com/International/europe-united-face-trumps-greenland-threats-tariffs-eu/story?id=129324420; Christensen, G. S., Hopkins, B. J., Bolin, N. B., & Allman, D. R. (2025). *Trump Administration Directs CFIUS to Tighten Restrictions on Investment From Certain Countries While Easing National Security Reviews of Investments From Allies and Partners* [US Policy and Regulatory Alert]. K&L Gates. https://www.klgates.com/Trump-Administration-Directs-CFIUS-to-Tighten-Restrictions-on-Investment-From-Certain-Countries-While-Easing-National-Security-Reviews-of-Investments-From-Allies-and-Partners-2-26-2025; Field, M. (2025, December 23). An Industry Guide to the FY2026 NDAA. *War on the Rocks*. https://warontherocks.com/cogs-of-war/an-industry-guide-to-the-fy2026-ndaa/; Gharagozlou, L. (2025, October 19). How Western sanctions on Iran have hurt the same middle class that drives reform. *CNN*. https://www.cnn.com/2025/10/19/middleeast/how-western-sanctions-iran-hurt-middle-class-intl; *President Trump Continues to Drive an American Manufacturing Boom*. (2025). The White House. https://www.whitehouse.gov/releases/2025/10/president-trump-continues-to-drive-an-american-manufacturing-boom/.

15 Karma, R. (2025, April 20). What If China Wins the Trade War? *The Atlantic*. https://www.theatlantic.com/economy/archive/2025/04/china-trump-trade-war/682524/.

16 Packard, C. (2023, October 12). Illiberalism Continues to Plague the Chinese Economy. *Cato Institute*. https://www.cato.org/blog/illiberalism-continues-plague-chinese-economy; Pham, P. (2018, March 20). Why Do All Roads Lead To China? *Forbes*. https://www.forbes.com/sites/peterpham/2018/03/20/why-do-all-roads-lead-to-china/.

17 *National Security Strategy of the United States of America*. (2025). The White House. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

18 National Defense Authorization Act for Fiscal Year 2026, no. S.2296, Senate (2025). https://www.congress.gov/bill/119th-congress/senate-bill/2296/text.

19 *Cyber Workforce*. (n.d.). Chief Information Officer U.S. Department of War. Retrieved June 5, 2026, from https://dodcio.defense.gov/Cyber-Workforce/; *DoD Supply Chain Risk Management Guidebook*. (2025, December 1). Warfighting Acquisition University. https://www.waru.edu/tools/dod-supply-chain-risk-management-guidebook; *OSC Critical Technology Areas*. (n.d.). U.S. Department of Defense. Retrieved June 5, 2026, from https://www.cto.mil/osc/critical-technologies/; *The Defense Department's Strategic and Critical Materials Review*. (2021). U.S. Department of Defense. https://www.war.gov/News/Releases/Release/Article/2649649/the-defense-departments-strategic-and-critical-materials-review/.
20 Miller, P. H. (2026, January 12). How the administration is preparing for the new economic Cold War. *The Hill*. https://thehill.com/opinion/national-security/5682848-wall-street-and-the-new-economic-cold-war/.
21 Farrell, H., & Newman, A. (2025, August 19). The Weaponized World Economy. *Foreign Affairs*, *104*(5). https://www.foreignaffairs.com/united-states/weaponized-world-economy-farrell-newman.
22 *Potomac Institute for Policy Studies*. (2025, October 10). Potomac Institute for Policy Studies. https://www.potomacinstitute.org/.
23 *Research*. (n.d.). Potomac Institute for Policy Studies. Retrieved June 5, 2026, from https://www.potomacinstitute.org/research.
24 Stevis-Gridneff, M., & Austen, I. (2026, January 20). Carney Speech on U.S. 'Rupture' and Canada's Survival Draws Standing Ovation at Davos. *The New York Times*. https://www.nytimes.com/2026/01/20/world/canada/carney-speech-davos-trump.html.

Chapter 1

25 *China: The Risk to Corporate America*. (2019). FBI. https://www.fbi.gov/file-repository/counterintelligence/china-risk-to-corporate-america-2019.pdf/view.
26 Welter, T., Norris, W., Blessing, J., & Stinson, J. (2025). *2025 Economic Statecraft Summit*. Potomac Institute for Policy Studies.
27 Sun Tzu. (2026). In *Britannica*. https://www.britannica.com/biography/Sunzi.
28 Liang, Q., & Xiangsui, W. (1999). *Unrestricted Warfare*. PLA Literature and Arts Publishing House.
29 Jie, Y., & Wallace, J. (2026, April 22). *What is China's Belt and Road Initiative (BRI)?* Chatham House. https://www.chathamhouse.org/2021/09/what-chinas-belt-and-road-initiative-bri; Sutter, K. M. (2026). *Made in China 2025 and China's Industrial Policies* (CRS No. IF10964). U.S. Congress. https://www.congress.gov/crs-product/IF10964.
30 *Military and Security Developments Involving the People's Republic of China*. (2025). U.S. Department of Defense. https://www.andrewerickson.com/wp-content/uploads/2025/12/China-Military-Power-Report_20251223.pdf.
31 CSET Original Translation: China's 14th Five-Year Plan. (2021, May 13). *Center for Security and Emerging Technology*. https://cset.georgetown.edu/publication/china-14th-five-year-plan/.
32 Karabell, Z. (2009). *Superfusion: How China and America Became One Economy and Why The World's Prosperity Depends on It* (1st Simon & Schuster ed). Simon & Schuster.
33 Skorup, J. (2014, January 2). The World Is Getting Better and Better. *Mackinac Center*. https://www.mackinac.org/the-world-is-getting-better.
34 Segal, A. (2017). *Chinese Cyber Diplomacy in a New Era of Uncertainty* (Aegis Paper Series 1703). Hoover Institution. https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.
35 *Four-Year Review of Actions Taken in the Section 301 Investigation: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*. (2024). Office of the United States Trade Representative. https://ustr.gov/sites/default/files/05.13.2024%20Four%20Year%20Review%20of%20China%20Tech%20Transfer%20Section%20301%20(Final)%20rev.pdf; *The China Initiative: Year-in-Review (2019-20)*. (2020). [Press Release]. U.S. Department of Justice. https://www.justice.gov/archives/opa/pr/china-initiative-year-review-2019-20.
36 Gilli, A., & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security*, *43*(3), 141–189. https://doi.org/10.1162/isec_a_00337.
37 *From High Tech to Heavy Steel: Combatting the PRC's Strategy to Dominate Semiconductors, Shipbuilding, and Drones*. (2024). http://chinaselectcommittee.house.gov/committee-activity/hearings/from-high-tech-to-heavy-steel-combatting-the-prc-s-strategy-to-dominate-semiconductors-shipbuilding-and-drones.
38 *Military and Security Developments Involving the People's Republic of China*, 2025.
39 Nomoko, S. (2025, July 24). Jihadists are intensifying drone attacks in the Sahel. *Le Monde*. https://www.lemonde.fr/en/international/article/2025/07/24/jihadists-are-intensifying-drone-attacks-in-the-sahel_6743662_4.html.
40 Kroenig, M., & Bayoumi, I. (2024). *A Global Strategy to Secure UAS Supply Chains*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-global-strategy-to-secure-uas-supply-chains/.
41 *Summary of the 2018 National Defense Strategy of The United States of America*. (2018). U.S. Department of Defense. https://media.defense.gov/2020/May/18/2002302061/-1/-1/1/2018-NATIONAL-DEFENSE-STRATEGY-SUMMARY.PDF.
42 Sutherland, M. D., & Sutter, K. M. (2020). *COVID-19: China Medical Supply Chains and Broader Trade Issues* (No. R46304). U.S. Congress. https://www.congress.gov/crs-product/R46304.
43 Kardon, I. B. (2025). *Examining the PRC's Strategic Port Investments in the Western Hemisphere and the Implications for Homeland Security*. Carnegie Endowment for International Peace. https://carnegieendowment.org/posts/2025/02/examining-the-prcs-strategic-port-investments-in-the-western-hemisphere-and-the-implications-for-homeland-security.
44 *2022 National Defense Strategy*. (2022). U.S. Department of Defense. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.
45 von Clausewitz, C. (2021). *On War* (J. J. G. Graham, Trans.; The Project Gutenberg EBook). https://www.gutenberg.org/files/1946/1946-h/1946-h.htm (Original work published 1874).
46 *2025 Annual Report to Congress*. (2025). U.S.-China Economic and Security Review Commission. U.S. Congress. https://www.uscc.gov/sites/default/files/2025-11/2025_Annual_Report_to_Congress.pdf.

47 *2022 National Defense Strategy*, 2022; *Critical Technology Areas*. (n.d.). DoW Research & Engineering, OUSW(R&E). Retrieved June 5, 2026, from https://www.cto.mil/cta/; *Intel and Trump Administration Reach Historic Agreement to Accelerate American Technology and Manufacturing Leadership*. (2025). [Press Release]. Intel. https://www.intc.com/news-events/press-releases/detail/1748/intel-and-trump-administration-reach-historic-agreement-to.
48 *2025 Annual Report to Congress*, 2025; Blevins, E. G., Kwon, Y. W., & Sutter, K. M. (2023). *Semiconductors and the CHIPS Act: The Global Context* (No. R47558). U.S. Congress. https://www.congress.gov/crs-product/R47558; *Reports*. (n.d.). Select Committee on the CCP. Retrieved June 5, 2026, from https://chinaselectcommittee.house.gov/documents/reports; Welter, T., Blessing, J., Norris, W., & Stinson, J. (2025). *2025 Economic Statecraft Summit Report*. Potomac Institute for Policy Studies. https://potomacinstitute.org/reports/2025-economic-statecraft-summit-report.
49 Adjusting Imports of Processed Critical Minerals and Their Derivative Products into the United States. (2026, January 14). *The White House*. https://www.whitehouse.gov/presidential-actions/2026/01/adjusting-imports-of-processed-critical-minerals-and-their-derivative-products-into-the-united-states/; *National Security Strategy of the United States of America*. (2025). The White House. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.
50 *Report to Congress on U.S.-Origin Technology that the Chinese Communist Party (CCP) is Using in the Military-Civil Fusion (MCF) Strategy of the PRC*. (2025). U.S. Department of State.
51 U.S. Government Accountability Office. (2010). *National Security: Key Challenges and Solutions to Strengthen Interagency Collaboration* (GAO-10-822T). U.S. Government Accountability Office. https://www.gao.gov/products/gao-10-822t; (2026). *Countering China: Agencies Provided Over $1 Billion but Have Not Assessed Overall Results of Projects* (GAO-26-107822). U.S. Government Accountability Office. https://files.gao.gov/reports/GAO-26-107822/index.html.
52 Countering China Economic Coercion Act, H.R. 5580, 117th Congress (2021). https://www.congress.gov/bill/117th-congress/house-bill/5580/text.
53 Atkinson, R. D. (2025). *Marshaling National Power Industries to Preserve America's Strength and Thwart China's Bid for Global Dominance*. Hamilton Center on Industrial Strategy. https://www2.itif.org/2025-power-industry-war.pdf.
54 Brady, A.-M. (2017). *Magic Weapons: China's political influence activities under Xi Jinping*. Wilson Center. https://www.wilsoncenter.org/sites/default/files/media/documents/article/magic_weapons.pdf.
55 *Military and Security Developments Involving the People's Republic of China*. (2025). U.S. Department of Defense. https://www.andrewerickson.com/wp-content/uploads/2025/12/China-Military-Power-Report_20251223.pdf.
56 China Arming Houthi Rebels in Yemen in Exchange For Unimpeded Red Sea Passage. (2025, January 2). *Foundation for Defense of Democracies*. https://www.fdd.org/analysis/2025/01/02/china-arming-houthi-rebels-in-yemen-in-exchange-for-unimpeded-red-sea-passage/; Salami. (2025, August 12). China Sends Houthis Dual-Use Technology to Boost Influence and Undercut the US. *Stimson Center*. https://www.stimson.org/2025/china-sends-houthis-dual-use-technology-to-boost-influence-and-undercut-the-us/.
57 Designating Cartels And Other Organizations As Foreign Terrorist Organizations And Specially Designated Global Terrorists. (2025, January 20). *The White House*. https://www.whitehouse.gov/presidential-actions/2025/01/designating-cartels-and-other-organizations-as-foreign-terrorist-organizations-and-specially-designated-global-terrorists/; *National Drug Threat Assessment 2024* (DEA-DCT-DIR-010-24). (2024). U.S. Department of Justice Drug Enforcement Agency. https://www.dea.gov/sites/default/files/2025-02/508_5.23.2024%20NDTA-updated.pdf.
58 Eliot, K., & Buss, J. (2026, March 5). Fighting an Economic War Without Fused Intelligence. *War on the Rocks*. https://warontherocks.com/fighting-an-economic-war-without-fused-intelligence/.
59 Norris, W. (2026, February 23). Economic Statecraft and the Federal Institutional Architecture. *War on the Rocks*. https://warontherocks.com/economic-statecraft-and-the-federal-institutional-architecture/.
60 Welter, T. (2023). The Concept of an Economic Warfare Operations Capability (EWOC). *STEPS: Science, Technology, Engineering, and Policy Studies*, *8*, 42–54.
61 Kellogg, M. (2026, April 16). Operationalizing Economic Statecraft: A New Imperative for the Pentagon. *War on the Rocks*. https://warontherocks.com/operationalizing-economic-statecraft-a-new-imperative-for-the-pentagon/.
62 Johnston, A. I. (1998). *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*. Princeton University Press; Taylor, P. (2013). *The Thirty-Six Stratagems: A Modern Interpretation Of A Strategy Classic*. Infinite Ideas; Zedong, M. (1965). On Protracted War. In *Selected Works of Mao Tse-tung* (Vol. 2). Foreign Languages Press.
63 Gilpin, R. (1981). *War and Change in World Politics*. Cambridge University Press. https://doi.org/10.1017/CBO9780511664267; Liff, A. P., & Ikenberry, G. J. (2014). Racing toward Tragedy? China's Rise, Military Competition in the Asia Pacific, and the Security Dilemma. *International Security*, *39*(2), 52–91.
64 Dunlap, C. (2008). Lawfare Today: A Perspective. *Faculty Scholarship*, 146–154; Kittrie, O. F. (2016). *Lawfare: Law as a Weapon of War*. Oxford University Press.
65 DeVore, M. R. (2012). Exploring the Iran-Hezbollah Relationship: A Case Study of how State Sponsorship affects Terrorist Group Decision-Making. *Perspectives on Terrorism*, *6*(4/5), 85–107; Salehyan, I., Gleditsch, K. S., & Cunningham, D. E. (2011). Explaining External Support for Insurgent Groups. *International Organization*, *65*(4), 709–744. https://doi.org/10.1017/S0020818311000233.

Chapter 2

66 Norris, W. J. (2025). Security Externalities: A Firm-Centric Theoretical Framework for Economic Statecraft: States, Firms and Geoeconomic Agency: The Role of Private Business in Contemporary Economic Statecraft and Security. *Law & Geoeconomics*, *1*(2), 175–213. https://doi.org/10.1163/29505720-bja00009.
67 *Executive Office of the President*. (n.d.). The White House. Retrieved June 5, 2026, from https://www.whitehouse.gov/eop/; *Organization of the National Security Council and Subcommittees*. (n.d.). The White House. Retrieved June 5, 2026, from https://www.whitehouse.gov/presidential-actions/2025/01/organization-of-the-national-security-council-and-subcommittees/.

68 *Home*. (n.d.-a). United States Trade Representative. Retrieved June 5, 2026, from https://ustr.gov/node/11425; *Office of Management and Budget*. (n.d.). The White House. Retrieved June 5, 2026, from https://www.whitehouse.gov/omb/; *Office of Science and Technology Policy*. (n.d.). The White House. Retrieved June 5, 2026, from https://www.whitehouse.gov/ostp/; *Office of the National Cyber Director*. (n.d.). The White House. Retrieved June 5, 2026, from https://www.whitehouse.gov/oncd/; *Presidential Departments*. (n.d.). The White House. Retrieved June 5, 2026, from https://www.whitehouse.gov/internships/presidential-departments/.

69 *Organization of the National Security Council and Subcommittees*. (n.d.). The White House. Retrieved June 5, 2026, from https://www.whitehouse.gov/presidential-actions/2025/01/organization-of-the-national-security-council-and-subcommittees/; Rollins, J. W. (2022). *The National Security Council: Background and Issues for Congress* (No. R44828). U.S. Congress. https://www.congress.gov/crs-product/R44828#:~:text=Interagency%20Policy%20Committees%20(IPCs).

70 *Home*. (n.d.-b). Office of Foreign Assets Control. Retrieved June 5, 2026, from https://ofac.treasury.gov/; *Home*. (2026, June 5). United States Department of the Treasury Financial Crimes Enforcement Network. https://www.fincen.gov/; *Terrorism and Financial Intelligence*. (2026, February 13). U.S. Department of the Treasury. https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence.

71 *Role of the Treasury*. (n.d.). Retrieved June 5, 2026, from https://home.treasury.gov/about/general-information/role-of-the-treasury.

72 *Home*. (n.d.-c). DARPA. Retrieved June 8, 2026, from https://www.darpa.mil; *Home*. (n.d.-d). Defense Technology Security Administration. Retrieved June 8, 2026, from https://www.dtsa.mil/SitePages/default.aspx; *Homepage*. (n.d.-a). OUSW Acquisition & Sustainment. Retrieved June 8, 2026, from https://www.acq.osd.mil/; *Policy Home*. (n.d.). Under Secretary of War for Policy. Retrieved June 8, 2026, from https://policy.war.gov/.

73 *GIES Home*. (n.d.). OUSW A&S. Retrieved June 8, 2026, from https://www.businessdefense.gov/gies/index.html; *Office of Strategic Capital (OSC)*. (n.d.). [DoW Research & Engineering, OUSW(R&E)]. Retrieved June 8, 2026, from https://www.cto.mil/osc/.

74 *National Defense Authorization Act for Fiscal Year 2026* (2025/2026; Legislation No. 119–39). (2025). U.S. Congress. https://www.congress.gov/committee-report/119th-congress/senate-report/39/1; *The Concept of an Economic Warfare Operations Capability (EWOC)*. (n.d.). Potomac Institute for Policy Studies. Retrieved June 8, 2026, from https://www.potomacinstitute.org/steps/index.php/issues/july-2023/the-concept-of-an-economic-warfare-operations-capability-ewoc.

75 *The Committee on Foreign Investment in the United States (CFIUS)*. (2026, February 13). U.S. Department of the Treasury. https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

76 *Federal Trade Commission*. (2026, February 13). Federal Trade Commission. https://www.ftc.gov/; *Homepage*. (2026, May 15). U.S. Department of Justice. https://www.justice.gov/; *Team Telecom*. (2023, September 11). U.S. Department of Justice National Security Division. https://www.justice.gov/nsd/team-telecom.

77 *Enforcement*. (n.d.). Bureau of Industry and Security. Retrieved June 8, 2026, from https://media.bis.gov//enforcement; *Export Administration Regulations*. (n.d.). Bureau of Industry and Security. Retrieved June 8, 2026, from https://media.bis.gov//regulations/ear/744#supplement-4-744; *Homepage*. (n.d.-b). Bureau of Industry and Security. Retrieved June 8, 2026, from https://media.bis.gov/; *Office of Export Enforcement*. (n.d.). Retrieved June 8, 2026, from https://www.bis.gov/OEE.

78 *International Trade Administration*. (n.d.). International Trade Administration. Retrieved June 8, 2026, from https://www.trade.gov/; *National Institute of Standards and Technology*. (2026, May 18). NIST. https://www.nist.gov/; *U.S. Bureau of Economic Analysis (BEA)*. (n.d.). U.S. Bureau of Economic Analysis (BEA). Retrieved June 8, 2026, from https://www.bea.gov/.

79 About Us — Bureau of Economic, Energy, and Business Affairs. (n.d.). *United States Department of State*. Retrieved June 8, 2026, from https://www.state.gov/about-us-bureau-of-economic-energy-and-business-affairs/.

80 *Embassy Deal Teams*. (n.d.). United States Department of State. Retrieved June 8, 2026, from https://www.state.gov/deal-teams/.

81 *Embassy Deal Teams*, n.d.

82 *Commodity Futures Trading Commission*. (2026, June 3). Commodity Futures Trading Commission. https://www.cftc.gov/; *Department of Energy*. (2026, June 4). U.S. Department of Energy. https://www.energy.gov/; *Department of Transportation*. (n.d.). Department of Transportation. Retrieved June 8, 2026, from https://www.transportation.gov/; *Federal Communications Commission*. (2026, June 3). Federal Communications Commission. https://www.fcc.gov/; *Home*. (n.d.-e). U.S. Federal Reserve. Retrieved June 8, 2026, from https://www.federalreserve.gov/default.htm; *Home*. (n.d.-f). EXIM. Retrieved June 8, 2026, from https://grow.exim.gov/iframe-customer-success-carousel-full-width; *U.S. National Science Foundation*. (2026, May 27). U.S. National Science Foundation. https://www.nsf.gov/; *USDA*. (n.d.). U.S. Department of Agriculture. Retrieved June 8, 2026, from https://www.usda.gov/.

83 Heitshusen, V. (2025). *Committee Types and Roles*. U.S. Congress. https://www.congress.gov/crs-product/98-241#:~:text=Structure%20of%20the%20Committee%20System.

84 *CFIUS Overview*. (2026, February 13). U.S. Department of the Treasury. https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview; *CFIUS Reports and Tables*. (2026, February 13). U.S. Department of the Treasury. https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-reports-and-tables; *The Trade Practitioner*. (n.d.). Squire Patton Boggs. Retrieved June 8, 2026, from https://www.tradepractitioner.com/.

85 *Office of Investment Security*. (n.d.). Office of Investment Security. Retrieved June 8, 2026, from https://www.trade.gov/about-us/office-investment-security.

86 *50 USC 4565: Authority to review certain mergers, acquisitions, and takeovers*. (n.d.). OLRC. Retrieved June 8, 2026, from https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title50-section4565&num=0&edition=prelim; *Executive Orders*. (2016, August 15). National Archives. https://www.archives.gov/federal-register/codification/executive-order/11858.html; *Title 31 of the CFR*. (n.d.). National Archives. Retrieved June 8, 2026, from https://www.ecfr.gov/current/title-31.

87 *Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States*. (2022, September 20). Federal Register.

88 Foreign Investment Risk Review Modernization Act of 2018, H.R.5841 (2018). https://www.congress.gov/bill/115th-congress/house-bill/5841/text.

89 Tarbert, H. P. (2020). Modernizing CFIUS. *The George Washington Law Review*, *88*(6), 1477–1524.

90 Licensing: Classify your item. (n.d.). Bureau of Industry and Security. Retrieved June 8, 2026, from https://media.bis.gov//licensing/classify-your-item; The Commerce Control List. (n.d.). Bureau of Industry and Security. Retrieved June 8, 2026, from https://media.bis.gov//regulations/ear/774#supplement-1-774.
91 *Export Administration Regulations*, n.d.
92 *Homepage*, n.d.-b.
93 Casey, C. A., & Kerr, P. K. (2021). *The U.S. Export Control System and the Export Control Reform Act of 2018* (No. R46814). U.S. Congress. https://www.congress.gov/crs-product/R46814; Sutter, K. M. (2025). *U.S. Export Controls and China: Advanced Semiconductors* (No. R48642). U.S. Congress. https://www.congress.gov/crs-product/R48642.

Chapter 3

94 *2025 National Security Strategy*, 2025.
95 Nellis, S., & Vengattil, M. (2020, July 24). Intel chip delay forces shift to using more outside factories, shares drop. *Reuters*. https://www.reuters.com/article/business/intel-chip-delay-forces-shift-to-using-more-outside-factories-shares-drop-idUSKCN24O2WJ/.
96 *Text - H.R.5841 - 115th Congress (2017-2018): Foreign Investment Risk Review Modernization Act of 2018*, (2018) (testimony of Robert [R-NC-9 Rep. Pittenger). https://www.congress.gov/bill/115th-congress/house-bill/5841/text.

Chapter 4

97 *NVIDIA Corporation (NVDA) Q2 2026 Earnings Call Transcript*. (2025, August 27). Seeking Alpha. https://seekingalpha.com/article/4817296-nvidia-corporation-nvda-q2-2026-earnings-call-transcript.
98 Karaahmetovic, V. (2025, October 28). *How much does a GW of data center capacity actually cost*. Investing.Com UK. https://uk.investing.com/news/stock-market-news/how-much-does-a-gw-of-data-center-capacity-actually-cost-4329740; *NVIDIA Corporation (NVDA) Q2 2026 Earnings Call Transcript*, 2025.
99 Data Centre Lifecycle Risk Management and Insurance Program in Asia: Everything you need to know. (n.d.). *MARSH*. Retrieved June 8, 2026, from https://www.marsh.com/content/marsh2/asia/my/en_my/industries/real-estate/insights/data-centre-lifecycle-risk-management-insurance-program-asia.html; *Emerging markets may be at the beginning of a multi-year run*. (2026, February 12). Bank of America. https://bofaglobalresearch.podbean.com/e/emerging-markets-may-be-at-the-beginning-of-a-multi-year-run/.
100 *Office of Strategic Capital (OSC)*, n.d.
101 *What we do*. (n.d.). NSSIF. Retrieved June 8, 2026, from https://www.nssif.gov.uk/about-us/what-we-do.
102 *Australian Government seeking proposals to co-invest in Aussie ingenuity through venture capital market*. (2026). [Media Release]. Australian Government: Defence Ministers. https://www.minister.defence.gov.au/media-releases/2026-02-18/australian-government-seeking-proposals-co-invest-aussie-ingenuity-through-venture-capital-market.
103 *The Nato Innovation Fund*. (n.d.). Nato Innovation Fund. Retrieved June 8, 2026, from https://www.nif.fund/.
104 Crane, K. W., Linck, E., Carioscia, S. A., & Lal, B. (2019). *Government Strategic Investment Funds* (Assessment of the Utility of a Government Strategic Investment Fund for Space, pp. 15–24). Institute for Defense Analyses. https://www.jstor.org/stable/resrep22819.6.
105 Beer, A. (2025, October 14). The National Reconstruction Fund's real challenge. *InnovationAus.Com*. https://www.innovationaus.com/the-national-reconstruction-funds-real-challenge/.
106 *Abu Dhabi Investment Authority*. (n.d.). ADIA. Retrieved June 8, 2026, from https://www.adia.ae/; *Mubadala in North America*. (n.d.). Mubadala Investment Company. Retrieved June 8, 2026, from https://www.mubadala.com/en-us; *Public Investment Fund*. (n.d.). PIF. Retrieved June 8, 2026, from https://www.pif.gov.sa/en/; *Qatar Investment Authority*. (n.d.). QIA. Retrieved June 8, 2026, from https://www.qia.qa/en/pages/default.aspx.
107 Bainbridge, A. (2023, November 17). How Australia Pension Funds are Becoming Global Force. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2023-11-17/how-australia-pension-funds-are-becoming-global-force.
108 *Government Pension Investment Fund*. (n.d.). Government Pension Investment Fund. Retrieved June 8, 2026, from https://www.gpif.go.jp/en; Hisahiro, K. (2024). *Japan's Strategic Interests in the Global South: Indo-Pacific Strategy*. https://www.csis.org/analysis/japans-strategic-interests-global-south-indo-pacific-strategy.
109 *JPMorganChase Launches $1.5 Trillion Security and Resiliency Initiative to Boost Critical Industries*. (2025). [Press Release]. JPMorgan Chase. https://www.jpmorganchase.com/newsroom/press-releases/2025/jpmc-security-resiliency-initiative.
110 *One, Big, Beautiful Bill Provisions*. (n.d.). Internal Revenue Service. Retrieved June 8, 2026, from https://www.irs.gov/newsroom/one-big-beautiful-bill-provisions.
111 *2026 Infrastructure Priority List*. (n.d.). Infrastructure Australia. Retrieved June 8, 2026, from https://www.infrastructureaustralia.gov.au/2026-infrastructure-priority-list; *Landmark Planning and Infrastructure Bill becomes law*. (2025). [Press Release]. Gov.Uk. https://www.gov.uk/government/news/landmark-planning-and-infrastructure-bill-becomes-law; Widodo, B. T., & Yujana, L. H. (2023). Introduction of National Strategic Projects. In *Infrastructure for Inclusive Economic Development Volume 2: Case Studies of Accelerated Projects*. Economic Research Institute for ASEAN and East Asia and Ministry of Finance, Indonesia. https://www.eria.org/uploads/04_Ch_1-Introduction.pdf.
112 Bennon, M., & Fukuyama, F. (2023, August 22). China's Road to Ruin. *Foreign Affairs*, *102*(5). https://www.foreignaffairs.com/china/belt-road-initiative-xi-imf.
113 *JBIC signs MOU with Overseas Private Investment Corporation of the U.S., Department of Foreign Affairs and Trade, and Export Finance and Insurance Corporation of Australia*. (2018). [Press Release]. Japan Bank for International Cooperation. https://www.jbic.go.jp/en/information/press/press-2018/1112-011585.html.
114 *Home*. (n.d.-g). Indo-Pacific Partnership for Prosperity. Retrieved June 8, 2026, from https://www.indopacificpartnership.org; Indo-Pacific Energy Security Ministerial and Business Forum. (2026, March 13). *U.S. Embassy & Consulates in Japan*. https://jp.usembassy.gov/indo-pacific-energy-security-forum/.
115 *2025 Quad Foreign Ministers' Meeting*. (2025). [Press Release]. U.S. Department of State. https://www.state.gov/releases/office-of-the-spokesperson/2025/07/2025-quad-foreign-ministers-meeting/; Froman, M. (2026, February 6). U.S., Allies Aim to Break China's Critical Minerals Dominance.

Council on Foreign Relations. https://www.cfr.org/articles/u-s-allies-aim-to-break-chinas-critical-minerals-dominance; United States-Australia Framework For Securing of Supply in the Mining and Processing of Critical Minerals and Rare Earths. (2025, October 20). *The White House*. https://www.whitehouse.gov/briefings-statements/2025/10/united-states-australia-framework-for-securing-of-supply-in-the-mining-and-processing-of-critical-minerals-and-rare-earths/.

116 Froman, 2026; *Week in Review: Project Vault and the U.S. Strategic Critical Mineral Reserve*. (2026). EXIM. https://www.exim.gov/news/week-review-project-vault-and-strategic-critical-mineral-reserve.

117 *172 countries and multiple candidate vaccines engaged in COVID-19 vaccine Global Access Facility*. (n.d.). WHO. Retrieved June 8, 2026, from https://www.who.int/news/item/24-08-2020-172-countries-and-multiple-candidate-vaccines-engaged-in-covid-19-vaccine-global-access-facility; *Home*. (n.d.-h). Nord Pool. Retrieved June 8, 2026, from https://www.nordpoolgroup.com/en/; *Home*. (n.d.-i). Asean Plus Three Emergency Rice Reserve (APTERR). Retrieved June 8, 2026, from https://www.apterr.org/; *IEA Member countries to carry out largest ever oil stock release amid market disruptions from Middle East conflict—News*. (2026). IEA. https://www.iea.org/news/iea-member-countries-to-carry-out-largest-ever-oil-stock-release-amid-market-disruptions-from-middle-east-conflict.

118 Fumi, A., & Jay, J. (2025). *Designing Adaptive Backbones: Organizational Choices to Enable Systems Change* (SSRN Scholarly Paper No. 5546339). Social Science Research Network. https://doi.org/10.2139/ssrn.5546339.

119 The private sector's growing role in strengthening sovereign resilience. (2026, January 13). *Macquarie Group*. https://www.macquarie.com/us/en/insights/the-private-sectors-growing-role-in-strengthening-sovereign-resilience-defence-capabilities.html.

120 *Southeast Asia Energy Outlook 2026*. (2026). International Energy Agency. https://www.iea.org/reports/southeast-asia-energy-outlook-2026.

121 *Asia-Pacific Data Center Market Size, Growth Report, Investments*. (2026). Arizton. https://www.arizton.com/market-reports/apac-data-center-market-analysis.

122 The National Grid Corporation of the Philippines operates the national transmission network under a concession in which the State Grid Corporation of China holds a 40 percent stake.

123 The bipartisan Strategic Subsea Cables Act of 2026, introduced in the House of Representatives in February 2026 by Representatives Joe Wilson and Gregory Meeks, would establish a dedicated interagency committee on subsea cables, expand State Department capacity, and mandate sanctions against those who intentionally damage undersea infrastructure. New trans-Pacific systems backed by Google and Meta, including Echo, Bifrost, and Apricot, have been routed through Indonesian and Philippine waters to avoid the South China Sea.

124 January 2026 Indo-Pacific investment convening; records on file with the author.

125 Cerberus Capital Management acquired the former Hanjin shipyard at Subic Bay in 2022 with United States government support.

126 *The private sector's growing role in strengthening sovereign resilience.* (2026, January 13). Macquarie Capital. https://www.macquarie.com/us/en/insights/the-private-sectors-growing-role-in-strengthening-sovereign-resilience-defence-capabilities.html.

127 *The private sector's growing role in strengthening sovereign resilience,* January 13, 2026.

Chapter 5

128 *The Federal Budget in The Fiscal Year 2024*. (2025). U.S. Congressional Budget Office. https://www.cbo.gov/system/files/2025-03/61181-Federal-Budget.pdf.

129 W. Norris, 2026.

130 *Planning, Programming, Budgeting & Execution Process (PPBE)*. (n.d.). Warfighting Acquisition University. Retrieved June 8, 2026, from https://www.waru.edu/acquipedia-article/planning-programming-budgeting-execution-process-ppbe.

131 *Air Force President's Budget FY25*. (2024, August 13). Financial Management and Comptroller. https://www.saffm.hq.af.mil/FM-Resources/Budget/Air-Force-Presidents-Budget-FY25/.

132 Why AI Companies May Invest More than $500 Billion in 2026. (2025, December 18). *Goldman Sachs*. https://www.goldmansachs.com/insights/articles/why-ai-companies-may-invest-more-than-500-billion-in-2026.

133 Keys, C. M. (2024). *FY2025 Budget Request: Department of Defense-Military (Subfunction 051)* (Legislation No. IN12447). U.S. Congress. https://www.congress.gov/crs-product/IN12447.

134 *Loss of U.S. KC-135 Over Iraq*. (2026). [Press Release]. U.S. Central Command. https://www.centcom.mil/MEDIA/PRESS-RELEASES/Press-Release-View/Article/4432850/loss-of-us-kc-135-over-iraq/; Scanlon, M. (2026, March 16). Iran missile strike damages five KC-135 tankers in Saudi Arabia, officials say. *Military Times*. https://www.militarytimes.com/news/your-military/2026/03/16/iran-missile-strike-damages-five-kc-135-tankers-in-saudi-arabia-officials-say/; Seligman, L., & Holliday, S. (2026, March 14). Five Air Force Refueling Planes Hit in Iranian Strike on Saudi Arabia. *The Wall Street Journal*. https://www.wsj.com/livecoverage/us-israel-iran-war-news-2026/card/five-air-force-refueling-planes-hit-in-iranian-strike-on-saudi-arabia-wHYFMW2YG3p0rwH3HaGU.

135 Catchpole, D. (2026, March 12). USAF general says Boeing has to fix tanker problems before US orders more. *Reuters*. https://www.reuters.com/business/autos-transportation/usaf-general-says-boeing-has-fix-tanker-problems-before-us-orders-more-2026-03-12/; Williams, S. Sgt. D. (2025, December 4). *100th KC-46A Pegasus delivered to Travis AFB*. Air Force. https://www.af.mil/News/Article-Display/Article/4348313/100th-kc-46a-pegasus-delivered-to-travis-afb/.

136 Top 10 U.S. Exports: Aircraft On Path To Lowest Ranking In Decades. (2022, October 15). *Forbes*. https://www.forbes.com/sites/kenroberts/2022/10/15/top-10-us-exports-aircraft-on-path-to-lowest-ranking-in-decades/.

137 https://www.safie.hq.af.mil/News/Article-Display/Article/4183729/the-path-to-the-blended-wing-body-demonstrator-is-reaching-new-heights/

138 Lamothe, D., Copp, T., & Robertson, N. (2026, March 27). U.S. uses hundreds of Tomahawk missiles on Iran, alarming some at Pentagon. *The Washington Post*. https://www.washingtonpost.com/national-security/2026/03/27/iran-war-tomahawk-missiles/.

139 Stockman, F. (2026, March 4). Iran's Drones Cost a Fraction of the U.S. Weapons Shooting Them Down. *The New York Times*. https://www.nytimes.com/2026/03/04/business/iran-shahed-drones-missiles-us-war.html.

140 Ruitenberg, R. (2026, January 20). Defense tech startups had their best funding year ever in 2025. *Defense News*. https://www.defensenews.com/industry/2026/01/20/defense-tech-startups-had-their-best-funding-year-ever-in-2025/.
141 W. Norris, 2026.
142 *Planning, Programming, Budgeting & Execution Process (PPBE)*, n.d.
143 Mitchum, M. (2026, April 6). Sharpening Signals and Reducing Noise for Better Defense Budgets. *War on the Rocks*. https://warontherocks.com/sharpening-signals-and-reducing-noise-for-better-defense-budgets/.
144 Both ends of that range show the pattern. F-35 procurement ran 44 aircraft in fiscal year 2025, a requested 24 in fiscal year 2026, 47 enacted, and a requested 85 in fiscal year 2027, of which only 32 are funded through base appropriations. Javelin ran 1,279 rounds in fiscal year 2024 at $360.7 million, roughly $300,000 each, then 450 rounds in fiscal year 2025 and 649 requested for fiscal year 2026. See *Fiscal Year (FY) 2026 Budget Estimates*. (2025). U.S. Department of Defense. https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2026/Discretionary%20Budget/Procurement/Missile%20Procurement%20Army.pdf; Losey, S. (2025, June 12). Air Force F-35 buy would be cut in half under Pentagon spending plan. *Defense News*. https://www.defensenews.com/air/2025/06/12/air-force-f-35-buy-would-be-cut-in-half-under-pentagon-spending-plan/; Scanlon, M. (2026, April 28). Pentagon's FY27 budget seeks 85 F-35s, but most ride on reconciliation. *Military Times*. https://www.militarytimes.com/news/pentagon-congress/2026/04/28/pentagons-fy27-budget-seeks-85-f-35s-but-most-ride-on-reconciliation/.
145 Roque, A. (2022, December 7). House, Senate defense authorizers agree to multi-year munitions buys. *Breaking Defense*. https://breakingdefense.com/2022/12/house-senate-defense-authorizers-agree-to-multi-year-muntion-buys/.
146 Cancian, M. F., & Park, C. H. (2026). *Last Rounds? Status of Key Munitions at the Iran War Ceasefire*. CSIS. https://www.csis.org/analysis/last-rounds-status-key-munitions-iran-war-ceasefire.
147 Marrow, M. (2025, August 1). Air Force surges munitions buys with $4.3B for JASSM and LRASM, $3.5B for AMRAAM. *Breaking Defense*. https://breakingdefense.com/2025/08/air-force-surges-munitions-buys-with-4-3-billion-for-jassm-and-lrasm-3-5-billion-for-amraam/.
148 Stone, M. (2026, July 30). US strikes $58.6 billion Patriot missile deal amid rising stockpile concerns. *Military Times*. https://www.militarytimes.com/industry/techwatch/2026/07/30/us-strikes-586-billion-patriot-missile-deal-amid-rising-stockpile-concerns/.
149 Easley, M. (2026, March 25). DOD inks agreement with Lockheed Martin aimed at accelerating Precision Strike Missile production. *DefenseScoop.* https://defensescoop.com/2026/03/25/army-precision-strike-missile-production-prsm-lockheed-martin/; *RTX's Raytheon partners with Department of War on five landmark agreements to expand critical munition production*. (2026, February 4). RTX Raytheon. https://www.rtx.com/news/news-center/2026/02/04/rtxs-raytheon-partners-with-department-of-war-on-five-landmark-agreements-to-exp.
150 South, T. (2026, July 15). Pentagon Announces Multiyear Deals for Affordable Cruise Missiles. *Air & Space Forces Magazine*. https://www.airandspaceforces.com/pentagon-announces-multiyear-deals-to-buy-thousands-of-affordable-cruise-missiles/
151 Novelly, T. (2026, June 10). 'A terrible risk': Senate appropriators dim prospects of another defense reconciliation bill. *Defense One*. https://www.defenseone.com/policy/2026/06/senate-appropriators-defense-reconciliation-bill/414080/; Roque, A., & Insinna, V. (2026, April 13). The Pentagon wants a 188 percent bump for missile procurement. Can industry deliver? *Breaking Defense*. https://breakingdefense.com/2026/04/the-pentagon-wants-a-188-percent-bump-for-missile-procurement-can-industry-deliver/.
152 Insinna, V. (2026, January 12). With the boom for solid rocket motors for missiles, a perilous crunch in the supply chain. *Breaking Defense*. https://breakingdefense.com/2026/01/with-the-boom-for-solid-rocket-motors-for-missiles-a-perilous-crunch-in-the-supply-chain/.

Chapter 6

153 Pusztaszeri, A. (2024). Why China's UAV Supply Chain Restrictions Weaken Ukraine's Negotiating Power. *CSIS*. https://www.csis.org/analysis/why-chinas-uav-supply-chain-restrictions-weaken-ukraines-negotiating-power.
154 Varenikova, M. (2026, March 11). Ukraine Reaches a Milestone: Making 'China-Free' Drones. *The New York Times*. https://www.nytimes.com/2026/03/11/world/europe/ukraine-drones-china.html.
155 America's Dangerous Pursuit of Critical-Mineral Dominance. (2026, February 26). *The Economist*. https://www.economist.com/leaders/2026/02/26/americas-dangerous-pursuit-of-critical-mineral-dominance?giftId=Mjg2M2ZjMmYtYWVlYy00ODEyLWE5ZjAtZTE4MzI2MDQ1ZjRl&utm_campaign=gifted_article.
156 Welter, T., & McWeeney, M. (2026a, February 5). Sun Tzu in the Supply Chain: The New Face of Economic War With China. *War on the Rocks*. https://warontherocks.com/sun-tzu-in-the-supply-chain-the-new-face-of-economic-war-with-china/.
157 *The Concept of an Economic Warfare Operations Capability (EWOC)*, n.d.
158 *Defense Innovation Unit*. (n.d.). Defense Innovation Unit. Retrieved June 9, 2026, from https://www.diu.mil/; *Office of Strategic Capital (OSC)*, n.d.; Pentagon headhunting Goldman, JPMorgan bankers for "Economic Defense Unit", Semafor reports. (2026, March 11). *Reuters*. https://www.reuters.com/business/finance/pentagon-headhunting-goldman-jpmorgan-bankers-economic-defense-unit-semafor-2026-03-11/.
159 Humpal, J. (2025, October 10). Supply Chains Are Critical Infrastructure. It's Time U.S. Policy Caught Up. *War on the Rocks*. https://warontherocks.com/supply-chains-are-critical-infrastructure-its-time-u-s-policy-caught-up/.
160 At a Glance: The U.S. Defense Industrial Base. (2026, January 27). *War on the Rocks*. https://warontherocks.com/cogs-of-war/at-a-glance-the-u-s-defense-industrial-base/.
161 *Latest BCI report reveals escalating supply chain disruptions drive increased tier mapping and insur*. (2024, October 2). BCI. https://www.thebci.org/news/supply-chain-disruptions-drive-increased-tier-mapping-and-insurance-uptake.html; McKinsey Global Supply Chain Leader Survey 2024 | McKinsey & Company. (2024, October 14). *McKinsey & Company*. https://www.mckinsey.com/capabilities/operations/our-insights/supply-chain-risk-survey-2024.

162 Mapp, N. J. and J. (2023, June 14). In the Dark: How the Pentagon's Limited Supplier Visibility Risks U.S. National Security. *War on the Rocks*. https://warontherocks.com/in-the-dark-how-the-pentagons-limited-supplier-visibility-risks-u-s-national-security/.
163 Michienzi, C. (2025, March 12). Finding Adversaries Hiding in the Defense Department's Supply Chains. *War on the Rocks*. https://warontherocks.com/finding-adversaries-hiding-in-the-defense-departments-supply-chains/.
164 Michienzi, 2025.
165 Michienzi, 2025.
166 Roy, D. (2025b, July 30). The U.S. Critical Minerals Dilemma: What to Know | Council on Foreign Relations. *Council on Foreign Relations*. https://www.cfr.org/articles/us-critical-minerals-dilemma-what-know; *TSMC Intends to Expand Its Investment in the United States to US$165 Billion to Power the Future of AI*. (2025, March 4). Taiwan Semiconductor Manufacturing Company Limited. https://pr.tsmc.com/english/news/3210.
167 Swanson, A., & Hirsch, L. (2025, June 15). 'Golden Share' in U.S. Steel Gives Trump Extraordinary Control. *The New York Times*. https://www.nytimes.com/2025/06/15/us/politics/golden-share-us-steel-nippon-trump.html.
168 Humpal, 2025.
169 *Acquisition Transformation Strategy*. (2025). U.S. Department of War. https://media.defense.gov/2025/Nov/10/2003819441/-1/-1/1/ACQUISITION-TRANSFORMATION-STRATEGY.PDF.
170 Eliot & Buss, 2026.
171 Lopez, C. T. (2026, February 13). *Department Seeks Counsel of Industry Leaders to Advance Arsenal of Freedom*. U.S. Department of War. https://www.war.gov/News/News-Stories/Article/Article/4405845/department-seeks-counsel-of-industry-leaders-to-advance-arsenal-of-freedom/.
172 Welter & McWeeney, 2026a.

Chapter 7

173 *2025 Federal Bureau of Investigation Internet Crime Report*. (2025). FBI. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.
174 Loten, A. (2026, February 19). Nation-State Hackers Hit Businesses for Commercial Edge. *Wall Street Journal*. https://www.wsj.com/articles/nation-state-hackers-hit-businesses-for-commercial-edge-d07865e0; Scherbina, A. (2024, May 3). How much do US businesses lose due to malicious cyber activity? [Text]. *The Hill*. https://thehill.com/opinion/cybersecurity/4641199-cyberattack-businesses-money-loss-malicious-cybersecurity/; Scherbina, A., & Schlusche, B. (2024). *The Effect of Malicious Cyber Activity on the US Corporate Sector*. American Enterprise Institute. https://www.aei.org/wp-content/uploads/2024/04/Scherbina-Schlusche-The-Effect-of-Malicious-Cyber-Activity-WP-April2024-updated.pdf?x97961.
175 *Microsoft Digital Defense Report 2025*. (2025). Microsoft. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=1, p. 43.
176 Liu, Y., Qiang, C. Z., Neto, A. M., Srinivasan, S., Khurana, S., Wang, H., & Porras, J. (2025). *Digital Progress and Trends Report 2025*. World Bank Group. https://openknowledge.worldbank.org/server/api/core/bitstreams/f2509a0f-7153-4f32-b180-bc11e90c4940/content.
177 *Annual Threat Assessment of the U.S. Intelligence Community*. (2024). Office of the Director of National Intelligence. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf; Rawlins, M., Tatsumi, Y., & Siebens, J. (2025). *Economic Coercion from the People's Republic of China*. Stimson Center. https://www.stimson.org/2025/economic-coercion-from-the-peoples-republic-of-china/.
178 Burton, J., & Lain, C. (2020). Desecuritising Cybersecurity: Towards a Societal Approach. *Journal of Cyber Policy*, *5*(3), 449–470. https://doi.org/10.1080/23738871.2020.1856903 ; Fruhlinger, J. (2020, February 12). The OPM Hack Explained: Bad Security Practices Meet China's Captain America. *CSO Online*. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html; Healey, J. (2011). *Pursuing Cyber Statecraft*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2011/09/091311_ACUS_PursuingCyber.pdf; Jaikaran, C. (2025). *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications* (In Focus No. IF12798). U.S. Congress. https://www.congress.gov/crs-product/IF12798; Limbago, A. L. (2015, July 1). *One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft*. National Defense University Press. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/607659/one-size-does-not-fit-all-the-multifaceted-nature-of-cyber-statecraft/; *NSA and Others Provide Guidance to Counter China State-Sponsored Actors Targeting Critical*. (2025, August 27). [Press Release]. National Security Agency/Central Security Service. http://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/; Welter, T., & McWeeney, M. (2026b, February 5). Sun Tzu in the Supply Chain: The New Face of Economic War With China. *War on the Rocks*. https://warontherocks.com/sun-tzu-in-the-supply-chain-the-new-face-of-economic-war-with-china/.
179 Jensen, B. (2023). How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy. *CSIS*. https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy.
180 Willett, M. (2019). Assessing Cyber Power. *Survival*, *61*(1), 85–90. https://doi.org/10.1080/00396338.2019.1569895.
181 Eliot & Buss, 2026; Hanson, N., & Field, M. (2026, January 29). Economic Statecraft Is Back. Is America Ready? *War on the Rocks*. https://warontherocks.com/economic-statecraft-is-back-is-america-ready/; W. Norris, 2026; Welter, Blessing, Norris, & Stinson, 2025; Welter & McWeeney, 2026b.
182 Hanson & Field, 2026.
183 *What is Cyber Statecraft?* (2026, June 9). RUSI. https://www.rusi.org.
184 Moore, D. (2022). *Offensive Cyber Operations: Understanding Intangible Warfare*. Oxford University Press.
185 *The Budget and Economic Outlook: 2025 to 2035*. (2025). Congressional Budget Office. https://www.cbo.gov/system/files/2025-01/60870-Outlook-2025.pdf.
186 Littmann, D., Fritz, J., Loucks, J., Stewart, D., Krause, T., & Joiner, C. (2025, February 20). *A New Metric for Tracking US Communications Infrastructure*. Deloitte Insights. https://www.deloitte.com/us/en/insights/industry/technology/us-communications-infrastructure-index.html; Mills, M. P. (2025). *The Rise of AI: A Reality Check on Energy and Economic Impacts*. National Center for Energy Analytics. https://energyanalytics.org/wp-content/uploads/2025/11/Mills_HAMM_AI_1125_Final_01.pdf.

187 Harry, C., & Gallagher, N. (2018). Classifying Cyber Events. *Journal of Information Warfare*, *17*(3), 17–31; Scissors, D. (n.d.). *China Global Investment Tracker*. American Enterprise Institute. Retrieved June 9, 2026, from https://www.aei.org/china-global-investment-tracker/; Wong, A. (2026, January 28). China's Economic Statecraft Is Working. *Foreign Affairs*. https://www.foreignaffairs.com/china/chinas-economic-statecraft-working.

188 Rotyburg, E. (2025, October 15). AI trading is Flooding Wall Street—And Fueling a 1.2 Trillion-Message Trading Surge, NYSE President Says. *Yahoo Finance*. https://finance.yahoo.com/news/ai-trading-flooding-wall-street-165840934.html.

189 *Fedwire Funds Service—Monthly Statistics*. (2026, May 19). The Federal Reserve. https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/monthly-stats.html.

190 *ACH Network Volume and Value Statistics*. (n.d.). Nacha. Retrieved June 9, 2026, from https://www.nacha.org/content/ach-network-volume-and-value-statistics.

191 Cipriani, M., Goldberg, L. S., & La Spada, G. (2023). *Financial Sanctions, SWIFT, and the Architecture of the International Payments System* (No. 1047). Federal Reserve Bank of New York; *Swift*. (n.d.). Swift. Retrieved June 9, 2026, from https://www.swift.com/homepage.

192 *Equifax Data Breach Settlement*. (2024, November). Federal Trade Commission. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement; Silver-Greenberg, J., Goldstein, M., & Perlroth, N. (2014, October 2). JPMorgan Chase Hacking Affects 76 Million Households. *The New York Times*. https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/; Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean? (2019, May 26). *Forbes*. https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/.

193 *Cost of a Data Breach Report 2025*. (2025). IBM, p. 12.

194 *Note by the President of the Security Council*. (2024). United Nations Security Council. https://docs.un.org/en/S/2024/215; Volz, D. (2023, August 4). WSJ News Exclusive | Crypto Heists Funneling Billions to North Korea's Nuclear Program Attract Senate Scrutiny. *Wall Street Journal*. https://www.wsj.com/politics/national-security/crypto-heists-funneling-billions-to-north-koreas-nuclear-program-attract-senate-scrutiny-698fd245.

195 Welter & McWeeney, 2026b.

196 Casey, C. A., Elsea, J. K., & Rosen, L. W. (2025). *The International Emergency Economic Powers Act: Origins, Evolution, and Use* (No. R45618). U.S. Congress. https://www.congress.gov/crs-product/R45618; Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113–291 (2014). https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf.

197 Biden, J. R. (2021). *Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation* (Executive Order No. 14024). The White House. https://www.federalregister.gov/documents/2021/04/19/2021-08098/blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the; Obama, B. (2016). *Executive Order 13757—Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities* [Executive Order]. Administration of Barack Obama. https://www.govinfo.gov/content/pkg/DCPD-201600880/pdf/DCPD-201600880.pdf; Trump, D. J. (2019). *Securing the Information and Communications Technology and Services Supply Chain* (Executive Order No. 13873). The White House. https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain; (2021). *Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber- Enabled Activities* (Executive Order No. 13984). The White House. https://www.federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.

198 *Cyber-Related Sanctions*. (2026, April 23). Office of Foreign Assets Control. https://ofac.treasury.gov/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities; *Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*. (2024). [Proposed Rule]. U.S. Department of Commerce. https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.

199 Gertz, G., & Kilcrease, E. (2025). *Publish an Economic Security Strategy*. CNAS. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Publish-an-Economic-Security-Strategy.pdf; McMaster, H. R., & Grotto, A. (2025). *Economic Statecraft: The Need For An Integrated Approach* [Essay]. Hoover Institution. https://www.hoover.org/research/economic-statecraft-need-integrated-approach.

200 Clark, J. (2024, January 12). *DOD Releases First Defense Industrial Strategy*. U.S. Department of War. https://www.war.gov/News/News-Stories/Article/Article/3644527/dod-releases-first-defense-industrial-strategy/; *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party*. (2023, December 12). Select Committee on the CCP. http://chinaselectcommittee.house.gov/media/policy-recommendations/reset-prevent-build-strategy-win-americas-economic-competition-chinese; *The Treasury 2021 Sanctions Review*. (2021). U.S. Department of Treasury. https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf.

201 Jones, C. (2025, May 10). Whiplash Reversals Mean Trump's Erratic Trade policy is as clear as mud. *The Guardian*. https://www.theguardian.com/us-news/2025/may/10/trump-tariffs-trade-policy-reversals.

202 *1998 Standard Occupational Classification Revision* (No. 150). (1998). Office of Management and Budget. https://www.bls.gov/soc/2000/frn-aug-5-1998.pdf; *Defending America's Cyberspace*. (2000). The White House. https://clintonwhitehouse5.archives.gov/media/pdf/npisp-fullreport-000112.pdf; Healey, J. (2023). Twenty-Five Years of White House Cyber Policies. *Lawfare*. https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies.

203 *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. (2009). The White House; National Security Archive. https://nsarchive.gwu.edu/document/21424-document-28; *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*.

(2011). The White House. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; *The White House, The National Strategy to Secure Cyberspace*. (2003). [Unclassified]. National Security Archive. https://nsarchive.gwu.edu/document/21412-document-16.

204 *Department of Defense Strategy for Operating in Cyberspace*. (2011). U.S. Department of Defense. https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf.

205 Alexander, D. (2014, March 28). Hagel, Ahead of China Trip, Urges Military Restraint in Cyberspace. *Reuters*. https://www.reuters.com/article/technology/hagel-ahead-of-china-trip-urges-military-restraint-in-cyberspace-idUSBREA2R1YO/; *The DoD Cyber Strategy*. (n.d.). U.S. Department of Defense; National Security Archive. https://nsarchive.gwu.edu/document/21384-document-25.

206 Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122; Valeriano, B., & Maness, R. C. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.

207 Davis, J. H., & Sanger, D. E. (2015, September 25). Obama and Xi Jinping of China Agree to Steps on Cybertheft. *The New York Times*. https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html; *Obama Threatens Sanctions Against China Over Cyber Hacking*. (2015, September 25). CBS News. https://www.cbsnews.com/news/obama-threatens-sanctions-against-china-over-cyber-hacking/; *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*. (2014, May 19). [Press Release]. U.S. Department of Justice. https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

208 Schelling, T. C. (2020). *Arms and Influence*. Yale University Press. https://yalebooks.yale.edu/book/9780300246742/arms-and-influence/ (Original work published 1966).

209 Lin, H. (2023). Where the New National Cybersecurity Strategy Differs From Past Practice. *Lawfare*. https://www.lawfaremedia.org/article/where-new-national-cybersecurity-strategy-differs-past-practice; Schneider, J. G. (2019). Deterrence in and through Cyberspace. In E. Gartzke, J. R. Lindsay, J. R. Lindsay, & E. Gartzke (Eds.), *Cross-Domain Deterrence: Strategy in an Era of Complexity* (p. 0). Oxford University Press. https://doi.org/10.1093/oso/9780190908645.003.0005; Smeets, M. (2025). *Ransom War: How Cyber Crime Became a Threat to National Security*. Oxford University Press.

210 Gertz & Kilcrease, 2025; Welter, Blessing, Norris, & Stinson, 2025, p. 12.

211 *National Cyber Strategy*. (2018). The White House; Trump White House. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

212 *Department of Defense Cyber Strategy 2018*. (2018). [Summary]. U.S. Department of Defense. https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf; Lonergan, E. (2023). Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior. *Lawfare*. https://www.lawfaremedia.org/article/operationalizing-defend-forward-how-concept-works-change-adversary-behavior.

213 *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. (2018). U.S. Cyber Command. https://www.cybercom.mil/portals/56/documents/uscybercom%20vision%20april%202018.pdf; Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, *45*(4), 534–567. https://doi.org/10.1080/01402390.2020.1732354.

214 Fischerkeller, M. P., Goldman, E. O., Harknett, R. J., & Nakasone, P. M. (2022). *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Oxford University Press. https://doi.org/10.1093/oso/9780197638255.001.0001; Stein, A. (2023, May 2). Are We Asking Too Much of Cyber? *War on the Rocks*. https://warontherocks.com/are-we-asking-too-much-of-cyber/.

215 *2023 Cyber Strategy*. (2023). [Summary]. U.S. Department of Defense. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf; Martelle, M. (2018). *Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL*. National Security Archive; Nakashima, E. (2019, February 26). U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. *The Washington Post*. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html; *National Cybersecurity Strategy*. (2023). The White House; Biden White House. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf; *President Trump's Cyber Strategy for America*. (2026). The White House. https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf.

216 Lyngaas, S. (2020, September 21). FBI hopes a more aggressive cyber strategy will disrupt foreign hackers. *CyberScoop*. https://cyberscoop.com/fbi-cyber-strategy-hackers-tonya-ugoretz/; *Shields Ready*. (n.d.). CISA. Retrieved June 16, 2026, from https://www.cisa.gov/shields-ready; *Shields Up*. (n.d.). CISA. Retrieved June 16, 2026, from https://www.cisa.gov/shields-up.

217 Eliot & Buss, 2026.

218 Nolan, A. (2015). *Cybersecurity and Information Sharing: Legal Challenges and Solutions* (No. R43941). Congressional Research Service. http://www.med.a51.nl/sites/default/files/pdf/R43941.pdf.

219 National Cybersecurity Protection Act of 2014, Pub. L. No. S.2519 (2014). https://www.congress.gov/bill/113th-congress/senate-bill/2519/text; Directorate for Information Analysis and Infrastructure Protection, 121 § 6 (2007). https://uscode.house.gov/view.xhtml?hl=false&edition=2006&req=granuleid%3AUSC-2012-title6-section121&num=0; *Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities*. (2013). https://www.congress.gov/event/113th-congress/house-event/LC857/text.

220 *Cyber Alert: The Cybersecurity Information Sharing Act Is Now Law*. (n.d.). Alston & Bird. Retrieved June 16, 2026, from https://www.alston.com/en/insights/publications/2015/12/icyber-alerti-the-cybersecurity-information-sharin.

221 Strohm, C. (2015, April 22). Companies Sharing Hacking Data Get Legal Shield in U.S. Bill. *Bloomberg*. https://www.bloomberg.com/news/articles/2015-04-22/companies-sharing-hacking-data-shielded-from-suits-in-house-bill.

222 *Home Page*. (n.d.). FOIA.Gov (Freedom of Information Act). Retrieved June 16, 2026, from https://www.foia.gov/.

223 Miller, J. (2013, June 13). DHS finds classified cyber sharing program slow to take off. *Federal News Network*. https://federalnewsnetwork.com/technology-main/2013/06/dhs-finds-classified-cyber-sharing-program-slow-to-take-off/.

224 Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 18 U.S.C. (1986); *FTC, DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information*. (2014, April 10). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity-information; Videnovic, A. F., Stefan. (2025, July 9). U.S. Cybersecurity at Risk Without Congressional Action. *FDD*. https://www.fdd.org/analysis/2025/07/09/u-s-cybersecurity-at-risk-without-congressional-action/.

225 Norris, W. (2025, May 14). *Empowering U.S. Economic Statecraft* [Testimony]. Economic Statecraft and Advancing US Interests Abroad, Washington D.C.

226 Cybersecurity Information Sharing Act, Pub. L. No. 114–113, 6 U.S.C. (2015). https://www.congress.gov/114/statute/STATUTE-129/STATUTE-129-Pg2242.pdf#page=695; Daniel, M. (2025). The Case for Reauthorizing CISA 2015. *Lawfare*. https://www.lawfaremedia.org/article/the-case-for-reauthorizing-cisa-2015.

227 Cybersecurity Information Sharing Act, Pub. L. No. 114–113, 6 U.S.C. (2015). https://uscode.house.gov/view.xhtml?req=(title:6%20section:1501%20edition:prelim)%20OR%20(granuleid:USC-prelim-title6-section1501)&f=treesort&edition=prelim&num=0&jumpTo=true#sourcecredit.

228 Agnew, K., Chiang, C. C., & Sprecher, C. (2025, August 27). The SEC Finalizes Rule on Cybersecurity Disclosures. *The CPA Journal*. https://www.cpajournal.com/2025/08/27/the-sec-finalizes-rule-on-cybersecurity-disclosures/; Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117–103, 6 U.S.C. (2022).

229 *Introduction to Information Sharing and Analysis Organizations* (No. 100–1). (2016). ISAO Standards Organization. https://www.isao.org/wp-content/uploads/2016/10/ISAO-100-1-Introduction-to-ISAO-v1-01_Final.pdf.

230 Karp, B. (2016, March 3). Federal Guidance on the Cybersecurity Information Sharing Act of 2015. *The Harvard Law School Forum on Corporate Governance*. https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.

231 Jaikaran, C. (2026). *The Cybersecurity Information Sharing Act of 2015: Expiring Provisions* (In Focus No. IF12959). Congressional Research Service. https://www.congress.gov/crs-product/IF12959.

232 W. Norris, 2026.

233 *DoD Cyberspace Operations: About 500 Organizations Have Roles, with Some Potential Overlap* (GAO-25-107121). (2025). U.S. Government Accountability Office. https://www.gao.gov/assets/gao-25-107121.pdf.

234 *About CISA*. (n.d.). CISA. Retrieved June 16, 2026, from https://www.cisa.gov/about; Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, 6 U.S.C. (2018). https://www.congress.gov/bill/115th-congress/house-bill/3359/text.

235 *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation* (GAO-21-236). (2021). U.S. Government Accountability Office. https://www.gao.gov/assets/gao-21-236.pdf#page=19; Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; *Information Sharing*. (n.d.). CISA. Retrieved June 16, 2026, from https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing; Simon-Lewis, A. (2017, May 19). This heat map shows how WannaCry spread around the world like an epidemic. *Wired*. https://www.wired.com/story/how-wannacry-spread-around-the-world/.

236 *Critical Infrastructure Sectors*. (n.d.). CISA. Retrieved June 16, 2026, from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors; *Joint Cyber Defense Collaborative*. (n.d.). CISA. Retrieved June 16, 2026, from https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative.

237 *CISA Central*. (n.d.). Retrieved June 16, 2026, from https://www.cisa.gov/about/cisa-central; *Stakeholder Engagement Division*. (n.d.). CISA. Retrieved June 16, 2026, from https://www.cisa.gov/about/divisions-offices/stakeholder-engagement-division.

238 *Connecting to the NICC and the NCCIC*. (2020, December 17). CISA. https://www.cisa.gov/resources-tools/resources/connecting-nicc-and-nccic; *Integrated Operations Division*. (n.d.). CISA. Retrieved June 16, 2026, from https://www.cisa.gov/about/divisions-offices/integrated-operations-division; *National Coordinating Center for Communications*. (n.d.). ISAO Standards Organization. Retrieved June 16, 2026, from https://www.isao.org/group/nccc/; *National Cybersecurity and Communications Integration Center (NCCIC)*. (n.d.). U.S. Department of Homeland Security. Retrieved June 16, 2026, from https://www.dhs.gov/keywords/national-cybersecurity-and-communications-integration-center-nccic.

239 *JCDC Success Stories*. (n.d.). CISA. Retrieved June 16, 2026, from https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-success-stories.

240 Doubleday, J. (2025, December 30). For DHS workforce, 2025 marked a year of major change. *Federal News Network*. https://federalnewsnetwork.com/hiring-retention/2025/12/for-dhs-workforce-2025-marked-a-year-of-major-change/; Geller, E. (2025b, October). *CISA's international, industry and academic partnerships slashed*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/cisa-stakeholder-engagement-division-layoffs-critical-infrastructure-international/803433/; Johnson, D. B. (2025, February 10). CISA Election, Disinformation Officials Placed on Administrative Leave, Sources Say. *CyberScoop*. https://cyberscoop.com/cisa-misinformation-disinformation-administrative-leave/; Starks, T. (2026, April 3). Trump Budget Proposal Would Cut Hundreds of Millions More from CISA. *CyberScoop*. https://cyberscoop.com/trump-budget-proposal-would-cut-hundreds-of-millions-more-from-cisa/; Wood, C. (2025, March 11). MS-ISAC Loses Federal Support for Threat Intelligence, Incident Response. *StateScoop*. https://statescoop.com/ms-isac-loses-federal-support/.

241 Blessing, J. (2020). *The Diffusion of Cyber Forces: Military Innovation and the The Diffusion of Cyber Forces: Military Innovation and the Dynamic Implementation of Cyber Force Structure* [Dissertation, Syracuse University]. https://surface.syr.edu/cgi/viewcontent.cgi?article=2191&context=etd#page=137.

242 *Command History*. (n.d.). U.S. Cyber Command. Retrieved June 16, 2026, from https://www.cybercom.mil/About/History/.

243 Nakashima, E. (2011, December 9). Cyber-intruder sparks response, debate. *The Washington Post*. https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

244 Blessing, J. (2025, January 29). Trump 2.0 and the Fracture of US Cyber Power. *Defense News*. https://www.defensenews.com/opinion/2025/01/29/trump-20-and-the-fracture-of-us-cyber-power/; Blessing, J., & Harknett, R. J. (2022). *The Advantage Gained: Building on USCYBERCOM-NSA's "Dual Hat" Synergy Model*. Kybernao. https://www.artsci.uc.edu/content/dam/refresh/artsandsciences-62/departments/political-science/ccsp/pdf_downloadableflyers/Kybernao_Issue2a.pdf.

245 Blessing, J. (2021). *The Global Spread of Cyber Forces, 2000–2018*. 13th International Conference on Cyber Conflict. https://doi.org/10.23919/CyCon51939.2021.9467807; Ferdinando, L. (2018, May 3). *Cybercom to Elevate to Combatant Command*. U.S. Department of War. https://www.war.gov/News/News-Stories/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/; Matishak, M. (2024, March 27). Exclusive: A high-level election security group is back. NSA and Cyber Command want to keep it under the radar. *The Record*. https://therecord.media/nsa-cyber-command-election-security-task-force-leaders-2024; Pomerleau, M. (2023, May 31). Five years in, a Look at How Cybercom and NSA's Integrated Cyber Center Improved Coordination of Operations. *DefenseScoop*. https://defensescoop.com/2023/05/31/five-years-in-a-look-at-how-cybercom-and-nsas-integrated-cyber-center-improved-coordination-of-operations/; (2025, July 1). Cyber Command significantly increases funding request for defense in Indo-Pacific region. *DefenseScoop*. https://defensescoop.com/2025/07/01/cyber-command-2026-budget-request-increase-funding-indo-pacific-defense/.

246 W. Norris, 2026.

247 *Investment Strategy for the Office of Strategic Capital*. (2025). U.S. Department of Defense. https://media.defense.gov/2025/Jan/02/2003623435/-1/-1/1/FY25-INVESTMENT-STRATEGY-FOR-OFFICE-OF-STRATEGIC-CAPITAL.PDF.

248 Desouza, K. C., & Fedorschak, K. (2015, February 3). The Vast Majority of the Government Lacks Clear Cybersecurity Plans. *Brookings*. https://www.brookings.edu/articles/the-vast-majority-of-the-government-lacks-clear-cybersecurity-plans/; *Office of the National Cyber Director*, n.d.; Riley, T. (2021, June 17). Chris Inglis Confirmed as First US National Cyber Director After Senate Vote. *CyberScoop*. https://cyberscoop.com/chris-inglis-national-cyber-director-senate-vote/.

249 *U.S. Cyberspace Solarium Commission*. (2020). U.S. Cyberspace Solarium Commission.

250 *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent*. (2023). Office of the National Cyber Director; Biden White House. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

251 *2024 Report on the Cybersecurity Posture of the United States*. (2024). Office of the National Cyber Director; Biden White House. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.

252 *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, 2021; Geller, E. (2025a, March 13). 'People Are Scared': Inside CISA as It Reels From Trump's Purge. *Wired*. https://www.wired.com/story/inside-cisa-under-trump/.

253 Nakashima, E. (2017, May 9). U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies. *The Washington Post*. https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html; Wehmeyer, J. (2024, December 20). Cyber Campaign Plans and Other Fairy Tales. *War on the Rocks*. https://warontherocks.com/cyber-campaign-plans-and-other-fairy-tales/.

254 *Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy* (GAO-24-106916). (2024). U.S. Government Accountability Office. https://www.gao.gov/assets/gao-24-106916.pdf; Klar, R., & Kagubare, I. (2023, April 4). Internal clashes reportedly led to White House cyber adviser's exit [Text]. *The Hill*. https://thehill.com/newsletters/technology/3934489-internal-clashes-reportedly-led-to-white-house-cyber-advisers-exit/; Scott, S. (2024). Counting the Costs in Cybersecurity. *Lawfare*. https://www.lawfaremedia.org/article/counting-the-costs-in-cybersecurity.

255 *Assessment of the Status of the Microelectronics Industrial Base in the United States*. (2023). U.S. Department of Commerce. https://www.bis.gov/media/documents/section-9904-report-final-20231221.pdf; *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities*. (2024). U.S. Government Accountability Office. https://www.gao.gov/assets/d24105563.pdf; Lockhart, F., & Lockhart, K. (2024). Harmonizing Cybersecurity Incident Disclosure After Loper Bright. *Lawfare*. https://www.lawfaremedia.org/article/harmonizing-cybersecurity-incident-disclosure-after-loper-bright; *Software Bill of Materials*. (n.d.). National Telecommunications and Information Administration. Retrieved June 16, 2026, from https://www.ntia.gov/page/software-bill-materials; Wehmeyer, J. (2025, August 13). Full Speed Ahead: Optimizing U.S. Cyber Command for the Future Fight. *War on the Rocks*. https://warontherocks.com/full-speed-ahead-optimizing-u-s-cyber-command-for-the-future-fight/.

256 Brands, H. (2014). *What Good Is Grand Strategy? By Hal Brands | Paperback*. Cornell University Press. https://www.cornellpress.cornell.edu/book/9780801456732/what-good-is-grand-strategy/.

257 *What Is an AI Model?* (2023, September 13). IBM. https://www.ibm.com/think/topics/ai-model.

258 *What Is a Frontier Model?* (n.d.). Cisco. Retrieved August 11, 2026, from https://www.cisco.com/site/us/en/learn/topics/artificial-intelligence/what-is-a-frontier-model.html.

259 *FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions*. (2024, November 13). U.S. Financial Crimes Enforcement Network. https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial; Menn, J. (2024, February 14). Microsoft, OpenAI say U.S. rivals use artificial intelligence in hacking. *The Washington Post*. https://www.washingtonpost.com/technology/2024/02/14/us-adversaries-using-artificial-intelligence-boost-hacking-efforts/; Stecklow, S., & McPherson, P. (2025, September 15). We wanted to craft a perfect phishing scam. AI bots were happy to help. *Reuters*. https://www.reuters.com/investigates/special-report/ai-chatbots-cyber/.

260 Google Threat Intelligence Group. (2025, November 6). *GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools*. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools.

261 Chia, O., & Cress, L. (2026, July 31). Anthropic's Claude AI escapes tests to hack three organisations. *BBC*. https://www.bbc.com/news/articles/cz7dl7w8y7po; Subin, S. (2026, August 1). OpenAI's Hugging Face hack confirmed months of AI cyber warnings: "Pandora's box is open." *CNBC*. https://www.cnbc.com/2026/08/01/open-ai-hugging-face-hack-cyber-warnings.html.

262 Sajadieh, S., Loredana, F., Raymond, P., Gil, Y., Parli, V., Santarlasci, L., Pava, J., Maslej, N., Altman, R., Brynjolfsson, E., Brodley, C., Clark, J., Dignum, V., Kumar, V., Landay, J., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., … Weld, D. (2026). *The AI Index 2026 Annual Report*. AI Index Steering Committee, Institute for Human-Centered AI. https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf.

263 *Are US Stock Market Valuations Outpacing Fundamentals?* (2026, July 10). Goldman Sachs. https://www.goldmansachs.com/insights/articles/are-us-stock-market-valuations-outpacing-fundamentals.

264 Buenaventura, M., Shenk, A., Nergui, A., Mann, S., Dolan, F. C., Patel, K. V., Mignano, J., & Welburn, J. W. (2025). *Artificial Intelligence Adoption and Sectoral Transformation: Implications for Health Care, Financial Services, Climate and Energy, and Transportation*. RAND. https://www.rand.org/pubs/research_reports/RRA3888-1.html.

265 Bowman, M. W. (2024, November 22). *Artificial Intelligence in the Financial System* [Speech]. 27th Annual Symposium on Building the Financial System of the 21st Century: An Agenda for Japan, Washington D.C. https://www.federalreserve.gov/newsevents/speech/bowman20241122a.htm; *Fraud is moving faster: How AI can help treasurers stay ahead*. (n.d.). US Bank. Retrieved August 11, 2026, from https://www.usbank.com/corporate-and-commercial-banking/insights/risk/mitigation/treasury-dept-partners-using-ai-to-fight-fraud.html; *Treasury Releases Report on the Uses, Opportunities, and Risks of Artificial Intelligence in Financial Services*. (2026, June 23). U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/jy2760; *U.S. Department of the Treasury Releases Report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Sector*. (2026, June 23). U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/jy2212.

266 Arnon, A. (2025). *The Projected Impact of Generative AI on Future Productivity Growth*. Penn Wharton Budget Model. https://budgetmodel.wharton.upenn.edu/p/2025-09-08-the-projected-impact-of-generative-ai-on-future-productivity-growth/; Filippucci, F., Gal, P., Jona-Lasinio, C., Leandro, A., & Nicoletti, G. (2024). The impact of Artificial Intelligence on productivity, distribution and growth: Key mechanisms, initial evidence and policy challenges. *OECD Artificial Intelligence Papers*. https://doi.org/10.1787/8d900037-en.

267 Constantin, L. (2025, February 7). Attackers hide malicious code in Hugging Face AI model Pickle files. *CSO Online*. https://www.csoonline.com/article/3819920/attackers-hide-malicious-code-in-hugging-face-ai-model-pickle-files.html; Montalbano, E. (2024, February 29). Hugging Face AI Platform Riddled With 100 Malicious Code-Execution Models. *Dark Reading*. https://www.darkreading.com/application-security/hugging-face-ai-platform-100-malicious-code-execution-models; *OWASP Top 10 for Large Language Model Applications*. (n.d.). OWASP Foundations. Retrieved August 11, 2026, from https://owasp.org/www-project-top-10-for-large-language-model-applications/; Tamari, S., & Tzadik, S. (2024, April 4). Hugging Face works with Wiz to strengthen AI cloud security. *Wiz*. https://www.wiz.io/blog/wiz-and-hugging-face-address-risks-to-ai-infrastructure; Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X., & Hamin, M. (2025). *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations* (NIST Artificial Intelligence (AI) 100-2 E2025). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-2e2025.

268 National Security Presidential Memorandum/NSPM-11. (2026, June 5). *The White House*. https://www.whitehouse.gov/presidential-actions/2026/06/national-security-presidential-memorandum-nspm-11/; Promoting Advanced Artificial Intelligence Innovation and Security. (2026, June 2). *The White House*. https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/; *Winning the Race: America's AI Action Plan*. (2025). The White House. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

269 Curi, M. (2026, May 19). Trump administration doubles down on Anthropic blacklisting in court arguments. *Axios*. https://www.axios.com/2026/05/19/anthropic-trump-administration-court-arguments.

270 Cai, S., & Haslett, C. (2026, June 13). Inside the whirlwind 24 hours that led the White House to slap export controls on Anthropic. *POLITICO*. https://www.politico.com/news/2026/06/13/inside-the-whirlwind-24-hours-that-led-the-white-house-to-slap-export-controls-on-anthropic-00961519; Isenstadt, A., & Curi, M. (2026, June 13). Scoop: Trump admin blocks foreign access to Anthropic's most powerful AI. *Axios*. https://www.axios.com/2026/06/12/anthropic-trump-mythos-fable-national-security.

271 Curi, M. (2026b, August 4). Scoop: Inside Trump's AI framework. *Axios*. https://www.axios.com/2026/08/04/trump-ai-framework-open-models.

272 Bessent, S. (2026, June 23). American Economic Statecraft in the 21st Century. In *U.S. Department of the Treasury* [Remarks]. Economic Club of New York's America 250 Gala Dinner, New York City, NY. https://home.treasury.gov/news/press-releases/sb0539.

273 Cai, S., & Haslett, C. (2026, June 13). Inside the whirlwind 24 hours that led the White House to slap export controls on Anthropic. *POLITICO*. https://www.politico.com/news/2026/06/13/inside-the-whirlwind-24-hours-that-led-the-white-house-to-slap-export-controls-on-anthropic-00961519.

274 Chorzempa, M. (2026, July 2). Fable of the Mythos saga: Ad hoc US AI model controls could help China. *PIIE*. https://www.piie.com/blogs/realtime-economics/2026/fable-mythos-saga-ad-hoc-us-ai-model-controls-could-help-china.

275 Mills, M. (2026, July 16). China's open-weight Kimi model stuns AI world with frontier-level results. *Axios*. https://www.axios.com/2026/07/16/moonshot-kimi-ai-china-model-openai-anthropic.

276 Goldman, E. O., & Grossman. (2026, July 6). Why Analytic Superiority Matters Most in the AI Race. *The National Interest*. https://nationalinterest.org/blog/techland/why-analytic-superiority-matters-most-in-the-ai-race.
277 *AI Cybersecurity Collaboration Playbook*. (2025, January 14). CISA. https://www.cisa.gov/resources-tools/resources/ai-cybersecurity-collaboration-playbook.
278 Barton-Cooper, R., & Gleave, A. (2026). AI Jailbreak Disclosure Is Broken. Here's How to Fix It. *AI Frontiers*. https://ai-frontiers.org/articles/ai-jailbreak-disclosure-is-broken-heres-how-to-fix-it; *CISA and Joint-Seal AI Publications*. (n.d.). CISA. Retrieved August 13, 2026, from https://www.cisa.gov/ai/cisa-products; Goel, S. (2026, August 3). Hugging Face CEO says hacks like the OpenAI episode needs transparency. *Business Insider*. https://www.businessinsider.com/hugging-face-ceo-hack-openai-mandatory-transparency-law-ai-2026-8; *Liability Rules and Standards*. (2024, March 24). National Telecommunications and Information Administration. https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report/using-accountability-inputs.

Chapter 8

279 Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017, May 18). Counter-Coercion Series: Senkaku Islands Trawler Collision. *Asia Maritime Transparency Initiative*. https://amti.csis.org/counter-co-trawler-collision/.
280 Welter, T., & McWeeney, M. (2026c, February 5). Sun Tzu in the Supply Chain: The New Face of Economic War With China. *War on the Rocks*. https://warontherocks.com/sun-tzu-in-the-supply-chain-the-new-face-of-economic-war-with-china/.
281 *Global Competitiveness of U.S. Advanced-Technology Manufacturing Industries: Communications Technology and Equipment* (Publication No. 2439). (1991). U.S. International Trade Commission. https://www.usitc.gov/publications/332/pub2439.pdf.
282 Hart, M., & Link, J. (2020, October 14). There Is a Solution to the Huawei Challenge. *Center for American Progress*. https://www.americanprogress.org/article/solution-huawei-challenge/.
283 Pongratz, S. (2025, October 9). Worldwide Telecom Equipment Revenue Up 4% in 1H25. *Dell'Oro Group*. https://www.delloro.com/worldwide-telecom-equipment-revenue-up-4-in-1h25/.
284 Atkinson, R. D. (2020). Who Lost Lucent?: The Decline of America's Telecom Equipment Industry. *American Affairs Journal*, *4*(3). https://americanaffairsjournal.org/2020/08/who-lost-lucent-the-decline-of-americas-telecom-equipment-industry/.
285 USCBC 2025 Member Survey: US-China Relations and Tariffs Are Primary Challenges for US Companies, but Staying in Market Is Essential to Remaining Globally Competitive. (2025, July 16). *The US-China Business Council*. https://www.uschina.org/news-releases/uscbc-2025-member-survey-us-china-relations-and-tariffs-are-primary-challenges-for-us-companies-but-staying-in-market-is-essential-to-remaining-globally-competitive/.
286 Clemens, E. (2026). *Internal Value Chains Remain Dependent on China Even as Multinationals Shift Production to America*. Information Technology and Innovation Foundation. https://itif.org/publications/2026/02/23/internal-value-chains-dependent-china-multinationals-shift-production-to-america/.
287 *To Stay Or To Go? What Speedy Supply Chain Relocation Means For Credit*. (2025). S&P Global Ratings. https://www.spglobal.com/ratings/en/regulatory/article/to-stay-or-to-go-what-speedy-supply-chain-relocation-means-for-credit-s101646958?
288 *DAF increases B-21 Raider production capacity to deliver combat capability faster*. (2026, February 23). Air Force. https://www.af.mil/News/Article-Display/Article/4412198/daf-increases-b-21-raider-production-capacity-to-deliver-combat-capability-fast/.
289 Rosenblatt, M. (2026b, May 26). Rebuilding American Manufacturing: A Keystone for Economic Statecraft. *War on the Rocks*. https://warontherocks.com/rebuilding-american-manufacturing-a-keystone-for-economic-statecraft/.
290 Keys, C. M. (2025). *FY2025 Department of Defense Appropriations: Status of Legislative Activity* (No. IN12402). Congressional Research Service. https://www.congress.gov/crs-product/IN12402.

Chapter 9

291 Tang, R. (2012). *China's Rare Earth Industry and Export Regime: Economic and Trade Implications for the United States* (No. R42510). Congressional Research Service. https://www.everycrsreport.com/files/20120430_R42510_8f135542e2ad4ef02a661779ee6793aa9db6a84c.pdf.
292 Sutter, K. M. (2019). *Trade Dispute with China and Rare Earth Elements* (In Focus No. IF11259). Congressional Research Service. https://www.congress.gov/crs-product/IF11259.
293 Amiti, M., Dai, M., Feenstra, R. C., & Romalis, J. (2017). *How Did China's WTO Entry Affect U.S. Prices?* (Working Paper No. 23487). National Bureau of Economic Research. https://doi.org/10.3386/w23487.
294 *Govini Data*. (n.d.). Rebuilding Manufacturing. Retrieved June 17, 2026, from https://rebuildingmanufacturing.com/.
295 Yao, K., & Jackson, L. (2025, November 10). China halts ban on gallium, germanium, antimony exports to US, but controls remain. *Reuters*. https://www.reuters.com/world/china/china-suspends-ban-exports-gallium-germanium-antimony-us-2025-11-09/.
296 *Chinese Cars Carve Out a Niche in Southeast Asia Dominated by Japanese Cars*. (2026, March 2). European Central Station. http://eu.36kr.com/en/p/3706376437936261; Palazzo, A., Hong, J., Torsoli, A., & Martin, M. (2026, February 2). One out of 10 Cars Sold in Europe Is Now Made by a Chinese Brand. *Claims Journal*. https://www.claimsjournal.com/news/national/2026/02/02/335426.htm; Parekh, N. (2026, September 3). *Chinese cars in Europe: A new vehicle fleet creating service potential*. S&P Automotive Insights. https://www.spglobal.com/automotive-insights/en/blogs/2026/03/chinese-cars-in-europe-vehicle-fleet-aftermarket; Tracy, D. (2024, May 3). I Drove A Bunch Of Chinese Cars And They Are Amazing: How China Learned To Build Better Cars While The West Was Sleeping. *The Autopian*. https://www.theautopian.com/i-drove-a-bunch-of-chinese-cars-and-they-are-amazing-how-china-learned-to-build-better-cars-while-the-west-was-sleeping/.
297 Treiss, F. (2026, March 16). BYD mulls new plant in Canada—And the acquisition of a global carmaker—Electrive.com. *Electrive*. https://www.electrive.com/2026/03/16/byd-mulls-new-plant-in-canada-and-the-acquisition-of-a-global-carmaker/.

298 Felton, R. (2026, May 9). China's Cars Aren't in the U.S., but Its Auto Parts Are Everywhere. *Wall Street Journal*. https://www.wsj.com/business/autos/chinas-cars-arent-in-the-u-s-but-its-auto-parts-are-everywhere-9fd408e5.

299 Soltani, E. (2025, April 17). *The Shift in Global Manufacturing Exports: U.S., Germany, and Japan Decline as China Rises*. Voronoi. https://www.voronoiapp.com/trade/-The-Shift-in-Global-Manufacturing-Exports-US-Germany-and-Japan-Decline-as-China-Rises-4764.

300 *2025 Annual Report to Congress*, 2025, pp. 472–536.

301 Tindale, C. (2026, January 16). *The case for emergency state capitalism starts with a simple point: National security sits upstream of every market outcome. A country that cannot make, refine, power, move, and repair the physical systems it depends can be remote controlled by a country that can. The* [Tweet]. Twitter. https://x.com/ctindale/status/2012130728545550450.

302 Facts About Manufacturing. (n.d.). *NAM*. Retrieved June 17, 2026, from https://nam.org/mfgdata/facts-about-manufacturing-expanded/.

303 Gaudiaut, T. (2025, December 8). *Infographic: China's Robotics Boom Leaves All Other Nations Behind*. Statista Daily Data. https://www.statista.com/chart/31337/operational-stock-and-new-installations-of-industrial-robots-by-country; Zhao, Y., Said, R., Ismail, N. W., & Hamzah, H. Z. (2024). Impact of industrial robot on labour productivity: Empirical study based on industry panel data. *Innovation and Green Development*, *3*(2), 100148. https://doi.org/10.1016/j.igd.2024.100148.

304 *Automation and the Work of the Future*. (2026, March 30). Manufacturing Renaissance. https://rebuildingmanufacturing.com/.

305 2026 Critical Minerals Ministerial. (2026, February 4). *United States Department of State*. https://www.state.gov/releases/office-of-the-spokesperson/2026/02/2026-critical-minerals-ministerial/; Hochman, T. (2025, September 5). Some Ideas for the Office of Strategic Capital. *Green Tape*. https://www.greentape.pub/p/some-ideas-for-the-office-of-strategic; Pax Silica. (n.d.). *United States Department of State*. Retrieved June 17, 2026, from https://www.state.gov/pax-silica/; Witte, C., & Becker, K. (2025, July 18). The One, Big, Beautiful Bill: Key insights for manufacturers. *Plante Moran*. https://www.plantemoran.com/explore-our-thinking/insight/2025/07/the-one-big-beautiful-bill-insights-for-manufacturers.

306 Empedocles, S. (2026, January 28). The missing middle: America's overlooked weakness in defense innovation. *Washington Technology*. https://www.washingtontechnology.com/companies/2026/01/missing-middle-americas-overlooked-weakness-defense-innovation/411017/; Frost, C. (2025, May 9). Don't Call Us Small: How the U.S. Can Support Its Own Mittelstand. *LinkedIn*. https://www.linkedin.com/pulse/dont-call-us-small-how-can-support-its-own-colin-frost-w7ibe/.

307 *Economic Data and Analysis*. (n.d.). Retrieved June 17, 2026, from https://rebuildingmanufacturing.com/.

308 Amiti, Dai, Feenstra, & Romalis, 2017.

309 Rosenblatt, M. (2024, November 12). Scale Drones to Win the Droid Market. *RealClearDefense*. https://www.realcleardefense.com/articles/2024/11/12/scale_drones_to_win_the_droid_market_1071532.html#_ftn1.

310 Boullenois, C., Black, M., & Caruso, A. (2026). *China's Next-Generation Industrial Policy*. Rhodium Group. https://rhg.com/research/chinas-next-generation-industrial-policy/.

311 Cervantes, M. (2026, January 30). Perú retira pedido para ingreso de buque hospital chino tras recomendación sanitaria. *China en las Américas*. https://chinalasamericas.com/2026/01/30/peru-retira-proyecto-buque-hospital-china-emergencia-sanitaria/; Cueto, C. (2026, March 4). *Chile suspende el proyecto Chile-China Express por riesgos geopolíticos*. DCD. https://www.datacenterdynamics.com/es/noticias/chile-suspende-cable-submarino-chino-por-riesgos-geopol%C3%ADticos/; McFields, A. (2026, March 25). China is losing ports, power and presence in Latin America [Text]. *The Hill*. https://thehill.com/opinion/international/5798196-chinese-influence-latin-america-decline/; Panama seizes two key ports from Hong Kong group amid U.S.-China canal dispute. (2026, February 24). *NBC News*. https://www.nbcnews.com/world/asia/panama-seizes-two-key-ports-hong-kong-group-us-china-canal-dispute-rcna260376.

312 O'Neil, S. (2026, March 26). The Donroe Doctrine Leans on Sticks But Needs Carrots. *Bloomberg*. https://www.bloomberg.com/opinion/articles/2026-03-26/trump-s-donroe-doctrine-won-t-win-latin-america-without-more-carrots.

313 Roy, D. (2025a, June 6). China's Growing Influence in Latin America | Council on Foreign Relations. *Council on Foreign Relations*. https://www.cfr.org/backgrounders/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri.

314 Kiryakova, E., Jackson, K., & Nadin, R. (2026). *China's economic footprint in Latin America and the Caribbean*. ODI Global. https://odi.org/en/publications/chinas-economic-footprint-in-lac/.

315 Ribeiro, P., & Chaudoin, N. (2025, August 21). China and Latin America Trade Deepens. *American Century Investments*. https://www.americancentury.com/insights/china-latin-america-trade-growth/.

316 *The Employment Situation—May 2026* (News Release USDL-26-0786). (2026). U.S. Bureau of Labor Statistics; *World Economic Outlook (April 2026)—Real GDP growth*. (2026, April). IMF. https://www.imf.org/external/datamapper/NGDP_RPCH@WEO.

317 *Equity Market Structure Archives*. (n.d.). SIFMA. Retrieved June 17, 2026, from https://www.sifma.org/issues/market-structure/equity-market-structure/; Neely, C. J., & Cole, A. (2026, February 25). *The U.S. Dollar's Role as a Reserve Currency*. Federal Reserve Bank of St. Louis. https://www.stlouisfed.org/open-vault/2026/feb/us-dollar-role-as-reserve-currency.

318 Aitken, T. (2026, May 10). The Forceful Ideology of Michael Pettis [Substack newsletter]. *Tom's Substack*. https://tomenergy.substack.com/p/the-forceful-ideology-of-michael.

319 Kellogg, 2026.

320 Two Cities, One Industry: US-Canada Auto Industry Took Generations to Build. (2025, December 22). *Detroit Regional Chamber*. https://www.detroitchamber.com/two-cities-one-industry-us-canada-auto-industry-took-generations-to-build/.

321 *Top Trading Partners—April 2026*. (2026). U.S. Census Bureau. https://www.census.gov/foreign-trade/statistics/highlights/topcm.html; Treiss, 2026.

322 Landes, A. (2026, April 6). *Ford Set to Release $30K Tesla-Killer in 2027*. Yahoo Autos. https://autos.yahoo.com/ev-and-future-tech/articles/ford-set-release-30k-tesla-160534916.html.

323 *S&P 500 Shareholder Returns*. (n.d.). Manufacturing Renaissance. Retrieved June 17, 2026, from https://rebuildingmanufacturing.com/.
324 Reif, L. R. (2026, April 1). America Is Losing the Innovation Race. *Foreign Affairs*. https://www.foreignaffairs.com/united-states/america-losing-innovation-race.
325 Burchell, B., & Hughes, A. (2006). *The Stigma of Failure: An International Comparison of Failure Tolerance and Second Chancing* (Working Paper No. 334). Centre for Business Research. https://www.jbs.cam.ac.uk/wp-content/uploads/2023/05/cbrwp334.pdf; *The Startup Ecosystem of United States*. (n.d.). Startup Blink. Retrieved June 17, 2026, from https://www.startupblink.com/startup-ecosystem/united-states.
326 *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*. (2018). Interagency Task Force. 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; *Production in the Innovation Economy (PIE)*. (n.d.). MIT. Retrieved June 17, 2026, from https://web.mit.edu/pie/.
327 *Decades of Manufacturing Decline and Outsourcing Left U.S. Supply Chains Vulnerable to Disruption*. (2022). [Bicameral Majority Staff Report]. Joint Economic Committee. https://www.cord-levin-center.org/server/api/core/bitstreams/5600a9ef-28d9-4b80-9459-df7d21fa9c71/content; *Taxes Were the Easy Part*. (n.d.). Manufacturing Renaissance. Retrieved June 17, 2026, from https://rebuildingmanufacturing.com/.
328 Empedocles, 2026.
329 *Govini Chinese Suppliers Data Table*. (n.d.). Manufacturing Renaissance. Retrieved June 17, 2026, from https://rebuildingmanufacturing.com/.
330 *Automation and the Work of the Future*, 2026.
331 Weijian, S. (2025, November 10). Unraveling China's Productivity Paradox. *Yicai Global*. https://www.yicaiglobal.com/news/unraveling-chinas-productivity-paradox.
332 Knight, M. (2025, August 26). The AI Robotics Revolution: From Japan's Factory Floors to America's Living Rooms. *LinkedIn*. https://www.linkedin.com/pulse/ai-robotics-revolution-from-japans-factory-floors-americas-knight-ld4zc/.
333 Park, K. (2026, April 5). In Japan, the robot isn't coming for your job; it's filling the one nobody wants. *TechCrunch*. https://techcrunch.com/2026/04/05/japan-is-proving-experimental-physical-ai-is-ready-for-the-real-world/.
334 Kemp, A. (2018, March 15). Taiichi Ohno: Hero of the Toyota Production System. *QAD Blog*. https://www.qad.com/blog/2018/03/taiichi-ohno-toyota-production-system; Nakamura, M., Sakakibara, S., & Schroeder, R. (1998). Adoption of Just-in-Time Manufacturing Methods at U.S.- and Japanese-Owned Plants: Some Empirical Evidence. *IEEE Transactions on Engineering Management*, *45*(3). https://blogs.ubc.ca/nakamura/files/2016/03/nakamura_ieee_1998.pdf.
335 Moynihan, L. (2026, March 20). Palantir CTO says artificial intelligence is key to reshoring American manufacturing. *New York Post*. https://nypost.com/2026/03/20/business/palantir-cto-says-artificial-intelligence-is-key-to-reshoring-american-manufacturing/.
336 Shriftman, J. (2025, May 6). The American Manufacturing Renaissance: A Market Map for Rebuilding U.S. Industry [Substack newsletter]. *Jonathan Shriftman*. https://shriftman.substack.com/p/the-american-manufacturing-renaissance.
337 Kim, K., Omarova, S. T., Algers, J., Furnaro, A., Marzán, C. F. R., Palladino, L., & Tucker, T. N. (n.d.). *Industrial Policy 2025: Bringing the State Back In (Again)*. Roosevelt Institute. https://rooseveltinstitute.org/wp-content/uploads/2024/02/4013_RI_IndustrialPolicyReport_2025.pdf.
338 *MISA*. (n.d.). Manufacturing Renaissance. Retrieved June 17, 2026, from https://rebuildingmanufacturing.com/.
339 *Mannie Mac*. (n.d.). Manufacturing Renaissance. Retrieved June 17, 2026, from https://rebuildingmanufacturing.com/.
340 *MERA*. (n.d.). Manufacturing Renaissance. Retrieved June 17, 2026, from https://rebuildingmanufacturing.com/.
341 Smith, C. (2026). *US Output: America's Productive Renaissance Rebuilding an Industrial System in a Constraint-Driven World*. Artisan Partners. https://www.artisanpartners.com/content/dam/documents/insights/vxus/Peak-Insights-US-Output-Americas-Productive-Renaissance-vXUS.pdf.
342 Damodaran, A. (n.d.). *Home Page*. Damodaran Online. Retrieved June 17, 2026, from https://pages.stern.nyu.edu/~adamodar/.
343 *Why Capital Fled Manufacturing*. (n.d.). Manufacturing Renaissance. Retrieved June 17, 2026, from https://rebuildingmanufacturing.com/.
344 *MISA*, n.d.
345 Garfinkle, A. (2026, March 27). *Business Loan Interest Rate Statistics: Average Rates Across Lender Types in 2026*. Crestmont Capital. https://www.crestmontcapital.com/blog/business-loan-interest-rate-statistics; Rosenblatt, M. (2026a, May). *Chinese Subsidies Compendium*. Manufacturing Renaissance. https://rebuildingmanufacturing.com/.
346 *Taxes Were the Easy Part*, n.d.
347 *Mannie Mac*, n.d.
348 Sechuga, M., & Pandol, H. H. (2026, February 18). *Qualified Small Business Stock (QSBS) Explained*. Carta. https://carta.com/learn/startups/tax-planning/qsbs/.
349 Ancheta, A. (2026, April 1). *C Corp Explained: Definition, Benefits, and Taxation Details*. Investopedia. https://www.investopedia.com/terms/c/c-corporation.asp; *S corporations*. (n.d.). Internal Revenue Service. Retrieved June 17, 2026, from https://www.irs.gov/businesses/small-businesses-self-employed/s-corporations.
350 *MERA*, n.d.
351 a16z. (2026, April 3). The Great Crew Change. *It's Time to Build*. https://www.a16z.news/p/the-great-crew-change.

Chapter 10

352 War by Other Ledgers Archives. (n.d.). *War on the Rocks*. Retrieved July 16, 2026, from https://warontherocks.com/category/special-series/war-by-other-ledgers/.
353 Thai, L., Beleche, T., & Oluwarantimi, A. (2025). *Understanding the Impact and Costs Associated with Medical Device Shortages During the COVID-19 Pandemic on Providers, Health Systems, Patients, and Manufacturers*. ASPE. http://aspe.hhs.gov/reports/impact-device-shortages-during-covid-19.
354 Bearman, G., Pryor, R., Vokes, R., Cooper, K., Doll, M., Godbout, E. J., & Stevens, M. P. (2020). Reflections on the COVID-19 pandemic in the USA: Will we be better prepared next time? *International Journal of Infectious Diseases*, *96*, 610–613. https://doi.org/10.1016/j.ijid.2020.05.059.
355 *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. (2018, September 6). [Press Release]. U.S.

Department of Justice; U.S. Department of Justice. https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

356 *Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)*. (2022, October 7). [Press Release]. Bureau of Industry and Security. https://www.bis.gov/press-release/commerce-implements-new-export-controls-advanced-computing-semiconductor-manufacturing-items-peoples.

357 *National Centers of Academic Excellence*. (n.d.). National Security Agency. Retrieved July 16, 2026, from https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/.

358 *The Human Genome Project*. (n.d.). National Institute of Health. Retrieved July 16, 2026, from https://www.genome.gov/human-genome-project.

359 Kharpal, A. (2026, January 26). Memory Chip Shortage to Last Through 2027, Semiconductor Boss Says. *CNBC*. https://www.cnbc.com/2026/01/26/memory-chip-shortage-synopsys-lenovo-ai-data-centers.html; Promoting Advanced Artificial Intelligence Innovation and Security. (2026, June 2). *The White House*. https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/.

360 CHIPS and Science Act, Pub. L. No. 117–167 (2022). https://www.congress.gov/bill/117th-congress/house-bill/4346.

361 *Economic Statecraft Program*. (n.d.). The Bush School of Government & Public Service. Retrieved July 16, 2026, from https://bush.tamu.edu/economic-statecraft/.

362 *Home*. (n.d.-j). Johns Hopkins SAIS. Retrieved July 16, 2026, from https://sais.jhu.edu/node/228413.

363 Yuzue, N., & Sekiyama, T. (2025). Defining economic security through literature review. *Frontiers in Political Science*, *7*. https://doi.org/10.3389/fpos.2025.1501986.

364 *Fox in the Henhouse*. (2025). House Select Committee on the CCP. http://chinaselectcommittee.house.gov/media/reports/fox-in-the-henhouse.

365 *Officer Professional Military Education Policy* (CJCSI 1800.01G). (2024). U.S. Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/education/cjcsi_1800.01g.pdf?ver=0coDQMMSkLNWpcg_prd9Gw%3D%3D.

366 Education & Training Center. (n.d.). *Hanscom AFB*. Retrieved August 13, 2026, from https://hanscomfss.com/education-training-center/.

367 Secretary of War. (2026a). *Rebuilding the Warrior Ethos in Professional Military Education* [Memorandum]. U.S. Department of War. https://media.defense.gov/2026/Feb/27/2003881803/-1/-1/1/REBUILDING-THE-WARRIOR-ETHOS-IN-PROFESSIONAL-MILITARY-EDUCATION.PDF; Note, this memo builds on Feb 6 2025 memo (2026b). *Aligning Senior Service College Opportunities with American Values* [Memorandum]. U.S. Department of War. https://media.defense.gov/2026/Feb/27/2003881802/-1/-1/1/ALIGNING-SENIOR-SERVICE-COLLEGE-OPPORTUNITIES-WITH-AMERICAN-VALUES.PDF.

368 *10 USC 9025: Office of Expanded Competition*. (2026, August 14). OLRC. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section9025&num=0&edition=prelim.

369 *2026 National Defense Strategy*. (2026). U.S. Department of War. https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF; *National Security Strategy of the United States of America*. (2025). The White House. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

370 Reference to DIME as an instrument of national power where D is diplomatic, I is informational, M is military, and E is economic.

371 *Economic Career Track*. (n.d.). U.S. Department of State. Retrieved August 13, 2026, from https://careers.state.gov/career-paths/foreign-service/foreign-service-officer/economic/; *Intelligence Analysis*. (n.d.). Intel.Gov. Retrieved August 13, 2026, from https://www.intelligence.gov/careers/explore-careers/intelligence-analysis; Kellogg, A. (2026, April 16). Operationalizing Economic Statecraft: A New Imperative for the Pentagon. *War on the Rocks*. https://warontherocks.com/operationalizing-economic-statecraft-a-new-imperative-for-the-pentagon/.

372 *Air University Catalog 2025-2026*. (2026). Air University. https://www.airuniversity.af.edu/Portals/10/Registrar/catalogs/AY26%20AU%20Catalog-Final%20Version-22-Jan-26.pdf?ver=yllmYAEb2jge_2EV-1N1Ow%3d%3d; *Programs and Courses*. (n.d.). National Defense University. Retrieved August 13, 2026, from https://www.ndu.edu/Academics/Programs-and-Courses/.

373 *International Officer School*. (n.d.). Air University. Retrieved August 13, 2026, from https://www.airuniversity.af.edu/IOS/; Sera, N. (2025, December 1). IOS marks 100 years of global partnership. *Air University*. https://www.maxwell.af.mil/News/Display/Article/4344965/ios-marks-100-years-of-global-partnership/.

374 Brown, C. (n.d.). *GASCC Keynote* [Keynote]. https://www.af.mil/Portals/1/documents/2022SAF/CSAF_Global_Air_Chiefs_Conference_readout.pdf.

375 *Home*. (n.d.). GigEagle. Retrieved August 13, 2026, from https://gigeagle.mil/.

376 Dartmouth Spotlights Economic Statecraft. (2025, April 23). *Dartmouth*. https://home.dartmouth.edu/news/2025/04/dartmouth-spotlights-economic-statecraft.

377 *Individual Mobilization Augmentee (IMA) Handbook*. (2024). U.S. Human Resources Command. https://www.hrc.army.mil/wcmt-api/sites/default/wcmtfiles/2024-11/Individual%20Mobilization%20Augmentee%20%28IMA%29%20Handbook%20-%20January%202024.pdf; Livermore, A. (2025, August 27). *The IMA program explained*. Air Force Life Cycle Management Center. https://www.aflcmc.af.mil/NEWS/Article/4287715/the-ima-program-explained/.

378 Huffman, T. (2017, May 8). *AF Reservist is leading scholar on Chinese military*. DVIDS. https://www.dvidshub.net/news/233002/af-reservist-leading-scholar-chinese-military; Mann, S. (2024, March 11). *Reserve Hypersonics Bullpen Taking Air Force Higher, Further, Faster*. Air Force Reserve Command. https://www.afrc.af.mil/News/Features/Display/Article/3687736/reserve-hypersonics-bullpen-taking-air-force-higher-further-faster/; *Oriana Skylar Mastro*. (n.d.). Stanford Freeman Spogli Institute for International Studies. Retrieved August 13, 2026, from https://fsi.stanford.edu/people/oriana-skylar-mastro.

Chapter 11

379 Hanson, N. & Field, M. (2026, January 29). Economic Statecraft Is Back. Is America Ready? *War on the Rocks*. https://warontherocks.com/economic-statecraft-is-back-is-america-ready/.

380 Harithas, B., Meng, K., Brown, E., & Mouradian, C. (2025). "Liberation Day" Tariffs Explained. *CSIS*. https://www.csis.org/analysis/liberation-day-tariffs-explained; Reddie, A., & Walker, L. (2025, July 15). Between Power and Promise: The Evolution of U.S. Sanctions Strategy. *IGCC*. https://ucigcc.org/blog/between-power-and-promise-the-evolution-of-u-s-sanctions-strategy/.

381 Heinrichs, R. L., & Sobolik, M. (2026, August 9). *America Is Too Dependent on Drugs from China. Worst-Case Scenario Could Be Disastrous*. Hudson Institute. https://www.hudson.org/supply-chains/america-too-dependent-drugs-china-worst-case-scenario-could-be-disastrous-rebeccah-heinrichs-michael-sobolik; Lincicome, S., & Anand, A. (2023). *The "China Shock" Demystified: Its Origins, Effects, and Lessons for Today*. CATO Institute. https://www.cato.org/publications/china-shock.

382 Bessent, S. (2026a, June 23). American Economic Statecraft in the 21st Century. In *U.S. Department of the Treasury* [Remarks]. Economic Club of New York's America 250 Gala Dinner, New York City, NY. https://home.treasury.gov/news/press-releases/sb0539; (2026b, June 23). Scott Bessent: Hamilton Inspires Trump's Economic Statecraft. *Wall Street Journal*. https://www.wsj.com/opinion/scott-bessent-hamilton-inspires-trumps-economic-statecraft-4a2786dd.

383 *The Bretton Woods Agreements*. (1944). [Act]. SDSU No Higher Law. https://loveman.sdsu.edu/docs/1944BrettonWoodsAgreement.pdf; Zerden, A., & Smith, L. (2024, April 12). Operationalizing a Doctrine for U.S. Economic Statecraft. *War on the Rocks*. https://warontherocks.com/operationalizing-a-doctrine-for-u-s-economic-statecraft/

384 Vincent, B. (2026, April 10). DOD officially launches new Economic Defense Unit to mesh military aims with global financial sway. *Defense Scoop*. https://defensescoop.com/2026/04/10/dod-economic-defense-unit-edu-steve-feinberg-pentagon/.

385 *NASCENT*. (n.d.). DARPA. Retrieved August 31, 2026, from https://www.darpa.mil/research/programs/nascent-national-security-economic-theory.

386 *A3ML. (n.d.). DARPA. Retrieved August 31, 2026, from https://www.darpa.mil/research/programs/a3ml-anticipatory-adaptive*.

387 Kellogg, A. (2026, April 16). Operationalizing Economic Statecraft: A New Imperative for the Pentagon. *War on the Rocks*. https://warontherocks.com/operationalizing-economic-statecraft-a-new-imperative-for-the-pentagon/.

388 Lyngaas, R., & Zerden, A. (2026). The Next Chapter of Treasury's War: Redefining a Department of Economic Security. *The Ledger*. https://theledgereconstatecraft.com/issues/issue-3/articles/the-next-chapter-of-treasurys-war-redefining-a-department-of-economic-security.html; Welter, T. (2023). The Concept of an Economic Warfare Operations Capability (EWOC). *STEPS: Science, Technology, Engineering, and Policy Studies*, 8, 42–55.

389 *10 USC 9025: Office of Expanded Competition*. (2026, August 14). OLRC. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section9025&num=0&edition=prelim.

390 National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119–60 (2025). https://www.congress.gov/bill/119th-congress/senate-bill/1071/text.

391 *About Us*. (n.d.). U.S.- China Economic and Security Review Commission. Retrieved August 31, 2026, from https://www.uscc.gov/about-us; *Comprehensive List of the Commission's 2025 Recommendations* (pp. 677–695). (2025). U.S.- China Economic and Security Review Commission. https://www.uscc.gov/sites/default/files/2025-11/2025_Comprehensive_List_of_Recommendations.pdf; Home. (2026, June 4). CECC. http://www.cecc.gov/.

392 *Issues*. (n.d.). Select Committee on the CCP. Retrieved August 31, 2026, from http://chinaselectcommittee.house.gov/issues.

393 Norris, W. (2026, February 23). Economic Statecraft and the Federal Institutional Architecture. *War on the Rocks*. https://warontherocks.com/economic-statecraft-and-the-federal-institutional-architecture/.

394 *Bills*. (n.d.). Select Committee on the CCP. Retrieved August 31, 2026, from http://chinaselectcommittee.house.gov/committee-activity/bills; *H.Res.11—Establishing the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party.*, (2023) (testimony of Kevin McCarthy). https://www.congress.gov/bill/118th-congress/house-resolution/11/text.

395 Sutherland, M. D., Benson, P. J., & Cho, C. Y. (2025). *TikTok: Frequently Asked Questions and Issues for Congress* (No. R48023). Congressional Research Service. https://www.congress.gov/crs_external_products/R/PDF/R48023/R48023.11.pdf.

396 Policy Alert: Codify the Pentagon's New Economic Defense Unit in the FY 2027 NDAA. (2026, June 10). *FDD Action*. https://www.fddaction.org/policy-alerts/2026/06/10/codify-pentagon-economic-defense-unit/.

397 Rosenblatt, M. (2026, May 26). Rebuilding American Manufacturing: A Keystone for Economic Statecraft. *War on the Rocks*. https://warontherocks.com/rebuilding-american-manufacturing-a-keystone-for-economic-statecraft/.

398 Skipper, G. (2026, March 25). Follow the Money: Finance and the Future of Allied Economic Statecraft. *War on the Rocks*. https://warontherocks.com/follow-the-money-finance-and-the-future-of-allied-economic-statecraft/.

399 Eliot, K., & Buss, J. (2026, March 5). Fighting an Economic War Without Fused Intelligence. *War on the Rocks*. https://warontherocks.com/fighting-an-economic-war-without-fused-intelligence/.

400 *Federal Acquisition Regulation*. (n.d.). Acquisition.GOV. Retrieved August 31, 2026, from https://www.acquisition.gov/browse/index/far.

401 Mitchum, M. (2026, April 6). Sharpening Signals and Reducing Noise for Better Defense Budgets. *War on the Rocks*. https://warontherocks.com/sharpening-signals-and-reducing-noise-for-better-defense-budgets/; Ray, G. (ret) T. (2026, April 30). Rethinking Corporate Risk and Alignment in an Era of Economic Statecraft. *War on the Rocks*. https://warontherocks.com/rethinking-corporate-risk-and-alignment-in-an-era-of-economic-statecraft/.

402 *Home*. (2022, January 26). Business Executives for National Security. https://bens.org/; Lopez, C. T. (2026, February 13). *Department Seeks Counsel of Industry Leaders to Advance Arsenal of Freedom*. U.S. Department of War. https://www.war.gov/News/News-Stories/Article/Article/4405845/department-seeks-counsel-of-industry-leaders-to-advance-arsenal-of-freedom/; *Office of Strategic Capital* (OSC). (n.d.). OUSW R&E. Retrieved September

1, 2026, from https://www.cto.mil/osc/; *Security and Resiliency Initiative*. (n.d.).

403 Blessing, J. (2026, April 23). Seeing the Cyber in Economic Statecraft. *War on the Rocks*. https://warontherocks.com/seeing-the-cyber-in-economic-statecraft/.

404 *Home*. (n.d.). Eisenhower School for National Security and Resource Strategy. Retrieved August 31, 2026, from https://es.ndu.edu/.

405 *Economic Statecraft Program* (Texas). (2025, August 5). The Bush School of Government & Public Service. https://bush.tamu.edu/research/programs/economic-statecraft/.

406 Buss, J. (2026, July 16). Academia's Critical Role in Developing an Economic Security Workforce. *War on the Rocks*. https://warontherocks.com/academias-critical-role-in-developing-an-economic-security-workforce/.

407 Kilcrease, E. (2026). *Hit It with Your Best Shot: An American Doctrine of Economic Pressure*. CNAS. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Sanctions-Doctrine_EES_Final_2026-03-31-225135_aoel.pdf

408 Dezenski, E. K., & Birenbaum, J. (2026). *A Gameplan for American Economic Security: Supercharging U.S. Statecraft, from an Economic Pentagon to the Near-Global Economy* [Memorandum]. Foundation for Defense of Democracies. https://www.fdd.org/analysis/2026/05/04/a-gameplan-for-american-economic-security-supercharging-u-s-statecraft-from-an-economic-pentagon-to-the-near-global-economy/.

409 Welter, T., Blessing, J., Norris, W., & Stinson, J. (2025). *2025 Economic Statecraft Summit Report*. Potomac Institute for Policy Studies. https://potomacinstitute.org/reports/2025-economic-statecraft-summit-report.

410 Muzinich, J. G., Raimondo, G. M., Taiclet, J. D., Hillman, J. E., & Schmemann, A. (2025). *U.S. Economic Security: Winning the Race for Tomorrow's Technologies* (Task Force Report No. 83). Council on Foreign Relations. https://www.cfr.org/task-force-reports/us-economic-security

411 Blessing, 2026; Rosenblatt, 2026; Welter, T., & McWeeney, M. (2026, February 5). Sun Tzu in the Supply Chain: The New Face of Economic War With China. *War on the Rocks*. https://warontherocks.com/sun-tzu-in-the-supply-chain-the-new-face-of-economic-war-with-china/.

412 Norris, 2026.

413 Eliot & Buss, 2026; Kellogg, 2026.

414 Buss, 2026; Ray, 2026.

Notes

Notes

Notes

Economics is a lever of national power, which has evolved into an active operational domain of current global competition and warfare.

That's why we have partnered with *War on the Rocks* on a collaborative series of webinars and articles — War by Other Ledgers.

This special series draws attention to how the U.S. can and should wield economic power to compete, coerce, and deter in an increasingly contested global order.

POTOMAC INSTITUTE FOR POLICY STUDIES

WAR ON THE ROCKS

901 N. Stuart Street, Suite 1200
Arlington, Virginia 22203
Phone: (703) 525-0770
Fax: (703) 525-0299
www.potomacinstitute.org



GLOBAL COMPETITION PROJECT