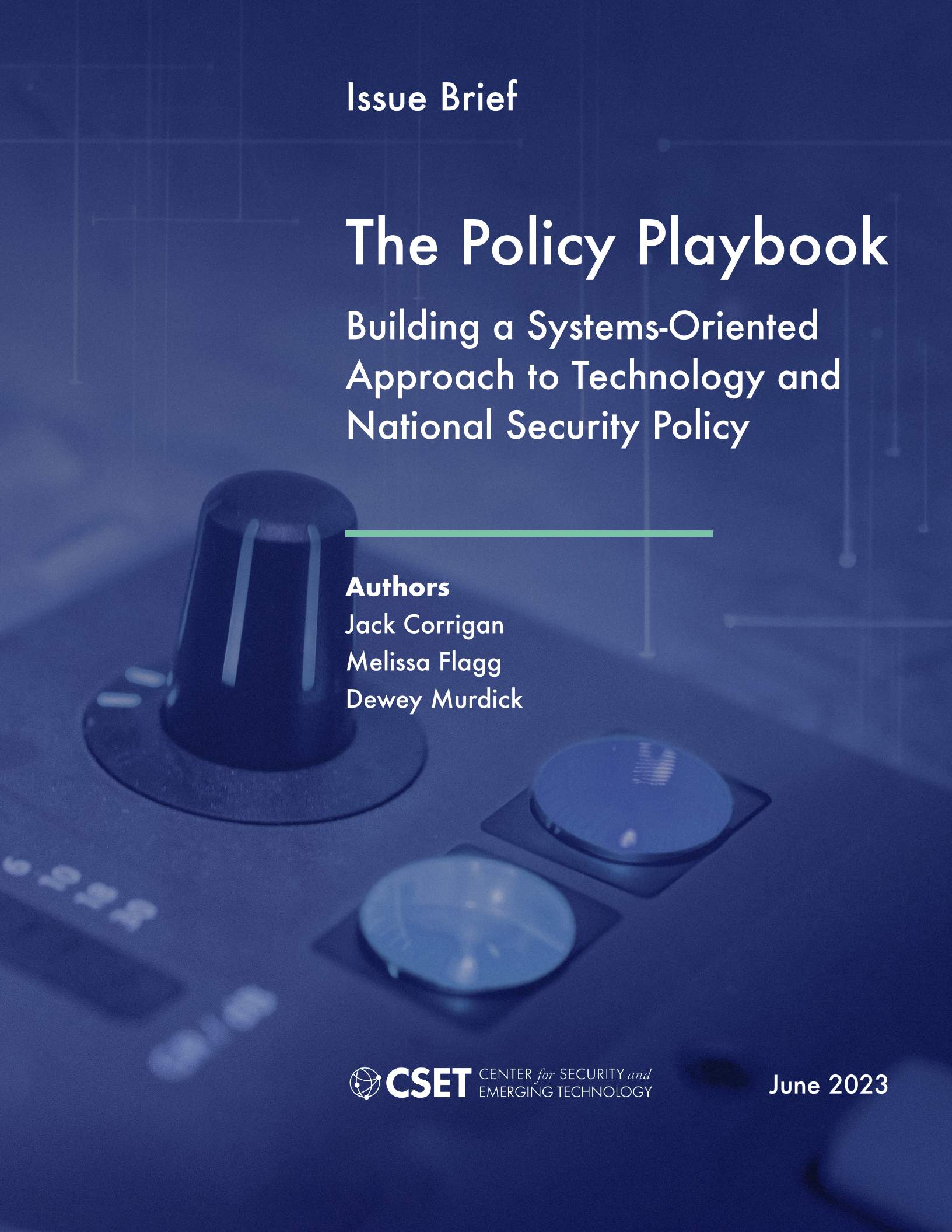
Issue Brief

The Policy Playbook

Building a Systems-Oriented Approach to Technology and National Security Policy

Authors
Jack Corrigan
Melissa Flagg
Dewey Murdick



CSET CENTER for SECURITY and EMERGING TECHNOLOGY

June 2023

Executive Summary

For leaders navigating the complexities of technology, national security, and the economy, the policy landscape can be quite disjointed and difficult to manage. Today's fragmented approach to policymaking—in which experts focus on narrow sets of issues and policies—can make it difficult to design holistic strategies, which often results in decisions that do not account for the complexity of the problems at hand. The government has a wide variety of policy levers at its disposal through which it can achieve its strategic goals. Understanding the interactions and tensions between these levers is critical to crafting an effective approach to emerging technology and national security.

This brief aims to provide a framework for a more systems-oriented technology and national security strategy. We begin by identifying and discussing the tensions between three strategic technology and national security goals:

1. **Driving technological innovation.**
2. **Impeding adversaries' progress**.
3. **Promoting safe, values-driven deployment.**

We go on to provide a brief overview of 15 levers of power through which policymakers can pursue these goals. These proposed levers fall into two categories: *direct levers of power* (there are nine), which are focused on discrete functions and issue sets; and *enabling levers of power* (there are six), which are more general-purpose and can be used to enhance the effect of the direct levers. These proposed categories are based on our own analysis, and while the list is non-exhaustive, it provides a useful framework for characterizing government actions and aligning them to particular goals of technology policy.

A more holistic, systems-oriented approach to policymaking is crucial for addressing novel challenges and balancing competing technology and national security goals. To craft effective strategies, leaders must understand the array of policy levers at their disposal, recognize the trade-offs, and create feedback mechanisms to monitor the real-time impacts of their policies in a rapidly changing world. This adaptable framework, suitable for any country or international body, emphasizes the importance of creative problem-solving and having a comprehensive understanding of the policy landscape to achieve strategic goals. This framework is intended for decision-makers and stakeholders in the realms of technology, national security, and economic policy.

Table of Contents

Executive Summary 1

Introduction 3

Strategic Technology and National Security Goals 4

- Goal 1: Drive Technological Innovation 5
- Goal 2: Impede Adversaries' Progress 6
- Goal 3: Promote Safe, Values-Driven Deployment 7

Tensions Among Goals 8

Government Levers of Power 10

- Direct Levers of Power 13
- Enabling Levers of Power 20
- Other Options 23

Conclusion 24

Authors 25

Acknowledgements 25

Endnotes 26

Introduction

For leaders navigating the complexities of technology, national security, and the economy, the policy landscape can be quite disjointed and difficult to manage. Policymakers may inadvertently rely on familiar levers or prioritize their agency's domain while overlooking the interconnectedness of various policy options that contribute to a cohesive strategy and defined goals. This approach to policymaking should not come as a surprise; the world is complicated, our institutions reward specialization, and spotting the links between different issues is not always easy. Experts tend to focus on narrow sets of issues and policies without fully grasping how they intersect and interact with others.[1] A fragmented approach to policymaking can make it difficult to design holistic strategies, and result in decisions that do not account for the complexity of the problems at hand. When researchers, analysts, and bureaucrats fixate on their preferred policy levers, the strategic forest can be lost for the trees.

The government has at its disposal a wide variety of policy levers, each optimized for different strategic goals.[2] When addressing the complex challenges of the 21st century, leaders need to comprehend this array of available tools, each with benefits and drawbacks that may be in tension when used together. Perhaps more importantly, policymakers would be wise to look beyond the current challenges and recognize how each policy lever will impact broader strategic goals that are all playing out in a dynamic, changing environment. As we will discuss later, these goals are often in tension with one another, and individual choices often advance certain goals while eschewing or even undermining others. While it would be ideal for the government to pursue every one of its policy goals in every situation, this is virtually impossible. To quote Harvard professor Michael Porter, "the essence of strategy is choosing what not to do. Without trade-offs, there would be no need for choices and thus no need for strategy."[3] Policymakers have the difficult responsibility of balancing these tensions and charting a measured, successful course for the country.

While applicable to all areas of public policy, this systems-oriented approach is especially pertinent in the realm of national security and emerging technology. The field is rife with internal tensions (e.g., innovation vs. security) and involves a variety of powerful interest groups with competing priorities. Additionally, given the breadth of the national security and emerging technology space, there are numerous policy levers that can be used to impact almost every part of society.

This enormous scope also exacerbates the problems of a policy-making environment that is optimized for individual policy outcomes. Virtually every government agency plays a role in shaping or responding to the domestic and international technology ecosystem, but each focuses on a subset of problems using a unique array of authorities. Narrowly optimized policies that lack high-level analysis and a deeper understanding of the levers options and interactions may end up not only attacking problems with the wrong tools, but often attacking the very solutions pursued by other agencies or destabilizing the broader policymaking ecosystem. You can drive a nail into a wall by hitting it with a screwdriver, but using a hammer is much more effective. Beyond using the right tool, policymakers must also ensure their actions are properly targeted. Regardless of the tool you use, driving a nail into the wrong part of the wall could result in a burst pipe, or worse.

Amid the global rise of authoritarianism, growing tensions with China, and rapid developments in emerging technologies such as artificial intelligence, government leaders often struggle with navigating the complex challenges at the speed of change. In this paper, we hope to provide a framework for a more coordinated, systems-oriented approach to understanding the policy mechanisms that can affect the technology and national security landscape and their associated tradeoffs. We begin by outlining three strategic goals of technology and national security policy; we then discuss the tensions and tradeoffs involved in pursuing those goals; and we conclude with an overview of 15 levers of power that government leaders can use to pursue these goals and construct a more systems-oriented policymaking environment. While this report focuses mostly on the U.S. policy ecosystem, we believe this framework can be adapted for virtually any country or international body.

Strategic Technology and National Security Goals

Within the United States, the federal government generally attempts to pursue strategies that ensure its military dominance, increase prosperity for the American people, and support the global norms that undergird free and open societies. Designing a successful technology and national security strategy, however, necessitates more concrete, actionable goals.

While the potential goals for such a strategy are numerous, many of the policy proposals recommended by the Center for Security and Emerging Technology and other well-regarded think tanks are aligned with three strategic goals:

1. **Drive technological innovation.**

2. **Impede adversaries' progress**.

3. **Promote safe, values-driven deployment.**

This list is not exhaustive, but rather a distillation of broad groups of technology and national security policy goals. Each goal comes with trade-offs, and no policy enacted in their pursuit will be effective in perpetuity. Given the dynamism of the geopolitical and economic landscape, government leaders need to create feedback loops to monitor emergent trends in technology policy, plan short- and long-term responses, recognize and respond to unintended consequences, and change course when tensions among goals fall out of balance.

Goal 1: Drive Technological Innovation

The first goal of an effective technology and national security strategy is to spur innovation. By enabling public and private innovators to "run faster," the United States can maintain its position on the cutting-edge of technology development and reap the rewards of global economic leadership.

Since World War II, the public sector has been a key driver of innovation in the United States. Many of today's foundational technologies, such as the internet, GPS, and mRNA platforms, trace their roots to government-funded research projects. But the government's involvement in the U.S. innovation ecosystem goes well beyond research and development (R&D) funding. Decisions related to infrastructure, education, immigration, taxes, trade, antitrust laws, intellectual property protections, and many other policy domains all impact the speed and trajectory of technological innovation. The impact of these instruments may vary across different technology sectors. For instance, in terms of innovation, nascent fields may benefit more from increased funding for basic research than tax credits to strengthen manufacturing, while the reverse would likely be true for more mature technology sectors.

In broad terms, pro-innovation policies typically support the generation, exchange, or application of new ideas. They may aim to increase the quantity or quality of R&D activity in particular areas; accelerate the deployment of new tools; reduce barriers to accessing knowledge and resources; or incentivize novel partnerships and collaborations. Generally, the goal of such policies is to accelerate the process by which new ideas, products, and systems enter the world.

The CHIPS and Science Act, passed in August 2022, is filled with examples of pro-innovation policies. These include new tax credits to incentivize companies to build chip manufacturing plants in the United States, billions of dollars in additional R&D funding, and investments in numerous workforce development programs, among others.[4] Some provisions focus on promoting particular types of innovation activities (e.g., reshoring semiconductor manufacturing), while others look to support technology development more indirectly (e.g., by strengthening STEM education).

Pro-innovation measures can create jobs, expand the economy, and produce groundbreaking discoveries, but they also have downsides. Novel technologies introduce new potential risks. Subsidies may entrench existing economic and political power structures. Reducing regulatory hurdles may accelerate technology deployment but it can also allow vulnerabilities to go unaddressed. It is not always wise to "move fast and break things." Policies to accelerate innovation must be supplemented with measures to promote safe and ethical technology deployment.

Goal 2: Impede Adversaries' Progress

Beyond empowering domestic innovators to "run faster," an effective technology and national security strategy also attempts to "slow down" the progress of potential adversaries. By obstructing its competitors, the United States can make up ground or sustain and expand its lead in critical technology sectors.

Efforts to impede adversaries' progress usually come to the fore during periods of great power competition.[5] During the Cold War, the United States used export controls and other trade restrictions to limit the Soviet Union's access to military and dual-use technologies.[6] Today, policymakers are employing similar tactics against China in response to the country's growing geopolitical clout and heavy reliance on industrial espionage, IP theft, and other extralegal trade practices.[7]

Policymakers can hinder competitors through both offensive and defensive measures. Offensive measures—which include policies such as export controls and sanctions—seek to limit potential adversaries' access to key technologies and resources in which the U.S. and its allies maintain an advantage. Such policies have historically targeted weapons and other military technology, but the October 2022 U.S. controls on semiconductor exports to China represent a shift toward a more broad-based crackdown on adversaries' technology development.[8]

Defensive measures, by contrast, aim to protect the United States against espionage, illicit technology transfer, or other nefarious activities undertaken by competitors to

advance their own interests or impede U.S. progress. The Federal Communications Commission's November 2022 order to ban U.S. sales of new equipment from Huawei and other foreign firms constitutes one such defensive measure.[9]

While policies to impede adversaries' progress can help the United States maintain its lead in strategic technologies, the efficacy of such measures may be limited. In our globalized economy, export controls and other related regimes are usually less effective without buy-in from allies.[10] Building this multilateral support can often prove challenging.[11] Furthermore, even when measures are properly implemented and enforced, their viability can diminish over time as technology progresses. Countries may find ways to circumvent technology controls, multilateral coordination may falter, and the potential costs of maintaining such measures may eventually outweigh the benefits.

Goal 3: Promote Safe, Values-Driven Deployment

An effective technology and national security strategy also implements guardrails to ensure new systems are functional, safe, and deployed in alignment with democratic values such as popular sovereignty, transparency, accountability, and the protection of rights and freedoms. These safeguards are necessary to prevent new technologies from causing intentional or inadvertent harm to the people, organizations, and societies that use them.

In the United States, policymakers have helped promote the safe deployment of new technologies since the early 20th century, when Congress enacted the first regulations on food and drug safety.[12] In the decades since, new advancements in technology have typically been followed by policies circumscribing how those tools should be designed and used. Typically, safety frameworks develop *after* a technology has already been deployed and its potential risks become clear.

Safety-related regulations typically fall into one of three buckets: **technology-based regulations**, which require technologies to include or exclude particular features (e.g., cars must have airbags); **performance-based regulations**, which set specific standards that a particular technology must meet (e.g., cars must achieve certain average fuel efficiency metrics); and **management-based regulations**, which require the creators of a technology to implement internal processes to ensure a socially desirable outcome (e.g. plant managers must conduct analysis and planning to reduce their use of toxic materials).[13]

Different types of regulations have their own strengths and weaknesses. For example, technology- and performance-based measures are relatively easy to enforce, but they

also leave it to the government to prescribe optimal performance thresholds and technology solutions, which might be mistargeted or slow to accommodate new technological developments. Management-based regulations allow markets and industry experts to work out optimal safety standards on their own, but they also rely on companies to sometimes make decisions that go against their financial interests.

Currently in national security circles, discussions about technology safety and ethics frequently center on artificial intelligence. Given the complexity and rapidly advancing applications of the AI field, few countries have implemented legally binding regulations on AI safety. However, there is an emerging consensus among the United States and its allies on the characteristics that "safe" AI systems would possess. These include explainability, transparency, accuracy, robustness, privacy protection, and lack of bias—all features that align with the values of free, open, and democratic societies.

A handful of countries and regions—including the United States, Japan, Canada, Australia, and European Union—have published "responsible AI" frameworks that generally align with these principles, as have international organizations such as the OECD and UNESCO.[14] Still, these frameworks are generally management-based, offering few specifics on how organizations should pursue these goals and what success would look like. Countries may endorse similar AI safety principles on paper, but in practice, their implementation of those principles will likely look very different.

Tensions Among Goals

Like many national governments around the world, the U.S. government is a complex organization composed of disparate agencies pursuing competing goals at the same time. For example, the National Science Foundation (NSF) supports cutting-edge research in an open system of intellectual merit while the Department of Defense (DOD) implements research security restrictions in that same ecosystem.[15] These countervailing forces combine to create the dynamic equilibrium that defines a country's overall technology strategy. This emergent strategy takes different forms in different countries. While governments generally pursue all three goals of technology and national security policy simultaneously, they tend to prioritize those goals differently depending on their political economy, the geopolitical landscape, and other factors.

For instance, consider the way the European Union and United States have each approached the process of developing responsible AI frameworks. Today, the EU is developing technical standards to measure AI systems for accuracy, robustness, transparency, and other characteristics.[16] Once implemented, these standards aim to

provide concrete, specific benchmarks for determining the safety and risks of AI systems, and help shape how they are deployed within the EU. Though some experts have questioned the viability of such standards, the EU's efforts represent the most significant attempt to regulate AI to date.[17] This effort will likely inform planning and implementation of future regulations.

Now compare this to the United States. For years, U.S. policymakers have discussed the need to deploy artificial intelligence in safe and ethical ways. The White House put forward executive orders to "promote the use of trustworthy AI," and national security leaders have spelled out the principles of responsible AI implementation in numerous speeches, reports, and strategy documents.[18] But to date, policymakers have taken relatively few steps in the way of creating binding AI safety regulations or technical standards. Instead, they appear to be relying largely on the private sector and the courts to develop guardrails for the technology.[19] At the same time, however, the U.S. government continues to devote significant resources to advancing the technology.[20]

This difference of approach underscores a key tension in technology policy: Safety regulations are often at odds with promoting innovation. Depending on their constraints and priorities, different countries—and even different government entities within the same country—strike different balances between these competing goals. The majority of companies on the cutting-edge of AI development are based in the United States, so it makes sense for U.S. leaders to favor pro-innovation policies over safety regulations. Doing so benefits domestic companies and protects the country's global leadership in technology. Similarly, it is reasonable for the EU and other countries to more vigorously pursue AI safety regulations.[21] These countries do not reap as many economic benefits from early deployments of AI, and implementing safety regulations allows them to play a role in shaping the trajectory of the technology.

Similar tensions frequently emerge in conversations about information security. Many of the cybersecurity challenges facing the world today stem from the fact that governments allowed digital networks to permeate almost every corner of society with little regard for security. In other words, we favored growth and innovation over safe deployment. Consider so-called "internet of things" devices, which are now ubiquitous across homes, offices, and public spaces in the United States. This technology has the potential to make our world more convenient, efficient, and inventive, but because the devices themselves often fail to meet even basic security standards, they also make our networked society more vulnerable to attacks. Numerous cybersecurity incidents, including the Mirai Botnet and Stuxnet, involved compromising network-connected devices.[22] In 2022, the United States and other countries proposed efforts to increase

IoT security through non-regulatory means like safety labels, but decades of forgoing safety for the sake of innovation have left policymakers playing catch-up.[23]

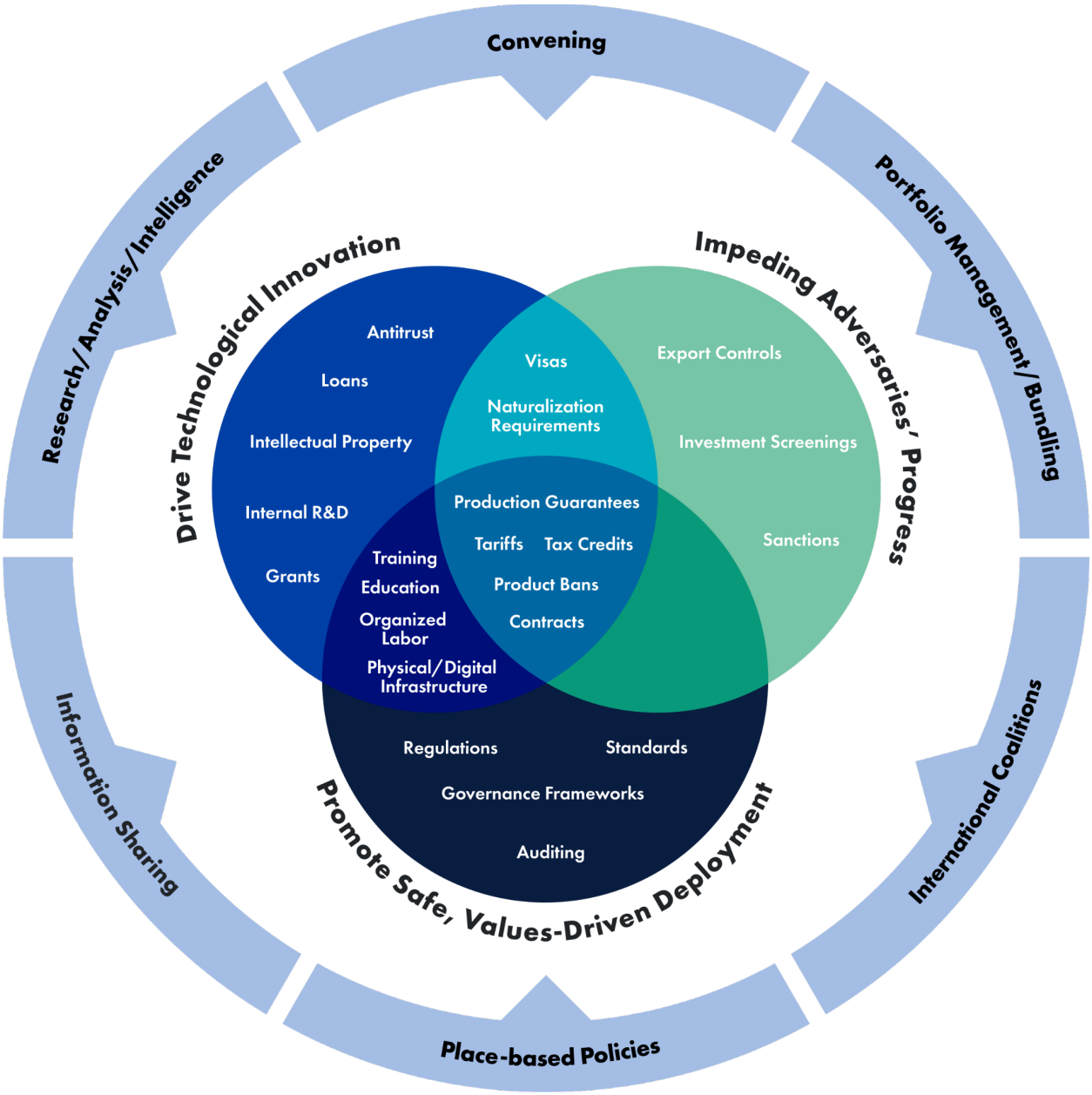
The technology policy landscape is rich with these sorts of tensions. Cooperative research partnerships can drive innovation while simultaneously helping adversaries advance their own technological capabilities.[24] Consolidating supply chains may create efficiencies that promote short-term innovation while undermining long-term resiliency and security. Export controls impede adversaries' progress but increase geopolitical tensions in ways that can hamper multilateral efforts to develop safety standards or promote innovation. Robust regulatory regimes promote safe deployment of technology while potentially pushing innovation activity to other, more lenient corners of the globe. Striking the right balance between these tensions is in many ways the primary purpose of government policy.

Government Levers of Power

Government policymakers have a variety of levers through which they can effect change and rebalance the tensions among different strategic goals. Each of these broad levers of power encompasses a range of specific policy instruments. For instance, one of the government's major levers of power as it relates to technology development is *Funding and Investment*, a category that includes instruments such as grants, subsidies, loans, and internal research and development programs (IRAD).

These levers of power may impact individual or multiple goals, and the nature of that impact can change depending on the specific structure and type of policy instruments that are used. Different levers may overlap and intersect in some cases, and certain policy instruments can be categorized under different levers, depending on how they are implemented. Figure 1 shows how certain policy instruments are aligned with one or more strategic technology and national security goals, and other levers can enable or amplify the effectiveness of different instruments.

Figure 1. Policy Instruments and Enabling Levers



In this section we provide an overview of 15 levers of power that government policymakers have at their disposal. These levers fall into two categories: *direct levers of power* (there are nine), which are focused on discrete functions and issue sets; and *enabling levers of power* (there are six), which are more general-purpose and can be used to enhance the effect of the direct levers. These proposed categories are based on our own analysis; there are many ways one might classify these levers of government

power. And while the list is non-exhaustive, it provides a useful framework for characterizing government actions and aligning them to particular goals of technology policy.

It is important to recognize that the popularity of particular policy levers and instruments tends to rise and fall over time; support for tariffs generally rises during periods of economic nationalism and falls during periods of globalization, for instance. While most of the examples in this section are rooted in the modern political landscape, we acknowledge the levers and instruments available to policymakers have varied widely over time, and the framework provided here is by no means static.

Direct Levers of Power

In this section, we describe nine direct levers of power through which government policymakers can pursue strategic technology and national security goals. Table 1 lists each direct lever of power along with examples of related policy instruments, and shows the strategic goals that we believe each lever is most closely aligned with.

Competition Policy

Competition is one of the most important drivers of innovation in capitalist economies, and the federal government's approach to *competition policy* can influence the type and trajectory of innovation across industries. When vying for customers, market share, and profits, firms are incentivized to reduce prices, adopt more efficient processes, and develop new and higher-quality products. Many innovation economists argue there is an "inverted U" relationship between innovation and competition; in markets with too much or too little competition, firms have less incentive to develop new products and processes.[25] Maintaining the right level of competition in key markets is therefore critical to driving technological development, and policymakers can play a meaningful role in striking this balance.

There are two primary instruments through which the federal government can impact firms' ability to compete with one another: intellectual property (IP) laws, which govern ownership of inventions, designs, and other works; and antitrust laws, which generally prohibit mergers, acquisitions, and business practices that harm competition. By reforming and selectively enforcing these laws, federal policymakers can affect the structure of various markets and change the incentives of firms. For instance, the 1956 consent decree against AT&T, which settled a longstanding government antitrust suit against the Bell System, required the lab to license thousands of patents to any applicant, royalty-free. The decision has been credited with giving rise to the commercial semiconductor industry and promoting innovation in a wide variety of other fields.[26] Since the late 20th century, the U.S. legal system has generally favored a combination of strong IP protections and weak antitrust enforcement.[27]

Table 1. Direct Government Levers of Power

Lever	Example Policy Instruments	Drive Innovation	Impede Adversaries	Promote Safe Deployment
Competition Policy	Intellectual property, antitrust	X		
Controls	Export controls, sanctions, investment screenings, foreign ownership restrictions		X	
Funding and Investment	Grants, subsidies, loans, internal R&D	X		
Immigration Policy	Visas, naturalization requirements	X	X	
Infrastructure	Public works, transportation, compute resources, research centers	X		X
Procurement	Production guarantees, contracts, requirements, product bans	X	X	X
Statutes, Regulations, and Standards	Consumer safety, governance, standards, auditing, insurance and liability		X	X
Taxes and Trade	Credits, tariffs, multilateral agreements, import quotas, antidumping penalties	X	X	X
Workforce Development*	Education, training, scholarships, civil rights, organized labor	X		X

**Federal policy is more of an "enabling" force in the education system, which is largely managed by state and local governments.*

Controls

The *controls* lever of power encompasses the various ways by which the U.S. government attempts to restrict the flow of capital, goods, and services between different countries. These efforts are typically intended to impede adversaries' progress, either by limiting their access to particular products and resources or by curtailing their participation in the global economy. Policy instruments that fall under this category include sanctions, export controls, end-user lists, and investment screenings. Given the United States' leadership in key sectors and the importance of the U.S. dollar in global financial markets, economic controls imposed by the U.S. government can have serious ramifications for their intended targets.

As of 2023, federal policymakers have embraced economic controls with renewed vigor amid the return to peer and near-peer competition. After its full scale invasion of Ukraine in February 2022, Russia was met with a slew of sanctions from the United States and its allies, which sent the country into a period of economic stagnation.[28] In October 2022, the United States introduced a set of expansive export controls intended to constrain China's semiconductor industry and, by proxy, its domestic AI ecosystem.[29] While economic controls can impede adversaries' progress in the short run, their long-term impacts are less clear cut. Restrictions such as export controls are usually only effective when enforced multilaterally, and it is not always easy to build this support among allies.[30] Furthermore, targeted countries can often find ways to evade controls, and in some cases, economic warfare harms the citizens of targeted countries more than the leaders whose behavior it is intended to sway.[31]

Funding and Investment

One of the federal government's most widely acknowledged levers of power is *funding and investment*, a broad category that encompasses the use of financial resources to support certain desired activities. Policy instruments such as research grants, investment programs, loan programs, targeted subsidies, and IRAD programs all fall into this category. In the context of technology and national security, funding and investment is particularly important for driving technological innovation. Today, the federal government accounts for roughly one-fifth of the country's total R&D spending, although in decades past the figure was significantly higher.[32]

Government funds play a significant role in supporting the country's talent pipeline through student loan programs. Other government funding programs are designed to compel particular behavior within the private sector. For instance, the CHIPS and

Science Act allocated $39 billion in subsidies for companies to construct new semiconductor fabrication facilities in the United States.[33] The Commerce Department began accepting applications for the subsidy program in February 2023.[34]

Immigration Policy

Another important lever of power in the context of technology and national security is *immigration policy*, which encompasses policies that impact the flow of foreign nationals into the United States and their socioeconomic prospects upon arriving. Immigrants comprise a significant share of the U.S. tech workforce, and many experts argue that increasing the flow of foreign-born technologists into the United States will be critical for maintaining the country's leadership in technologies like AI.[35] In this context, visa programs, naturalization requirements, and other immigration policy instruments can be designed to drive technological innovation by allowing the world's best and brightest to contribute to the U.S. tech ecosystem. Consider the Optional Practical Training (OPT) program, which allows international students on F-1 student visas to work temporarily in the United States after graduating. While every student can work for up to one year on OPT , those who earned STEM degrees are eligible for three years of employment.[36] By increasing the supply of STEM talent and giving graduates more opportunities to acquire work, employment-based visas and green cards, the program expands the U.S. tech workforce and drives innovation.

Immigration policy can also impede adversaries' progress. If talent is considered a zero-sum game, then attracting immigrants from adversarial nations strengthens the U.S. technical workforce while weakening the workforce of the other country. However, if the influx of foreign-born talent crowds U.S. workers out of certain lucrative fields, those domestic workers may become more economically vulnerable, which contributes to a wide range of destabilizing factors.

Infrastructure

Infrastructure initiatives are also a key lever of power that policymakers have at their disposal. In our definition, infrastructure programs encompass efforts to construct and maintain facilities, systems, and resources that undergird American society and the economy. While these programs often combine policy instruments from other levers of power—such as funding and investment, regulations, and taxes—infrastructure is such a uniquely governmental function that we classify it as its own lever of power. In the context of technology and national security, infrastructure initiatives can drive innovation by creating an environment in which organizations can operate more

reliably, efficiently, and effectively. For instance, increasing resiliency in the power grid helps businesses avoid disruptions in manufacturing, compute access, and other critical processes. Historic government-led infrastructure initiatives such as the Rural Electrification Act, which expanded the power grid beyond urban areas, and the Federal-Aid Highway program, which built the interstate highway system, helped galvanize the country's economic growth and cement its technological leadership in the 20th century.[37]

Other initiatives—such as roads designed to handle self-driving cars and electric vehicle charging networks—may also enable safer deployments of new technology. Digital infrastructure, such as the National Artificial Intelligence Research Resource (NAIRR), can also empower innovators and enable developers to produce new and safer technologies.

Procurement

Policymakers can also exercise significant influence over the technology and national security landscape through *procurement* decisions, or the government's purchase of goods and services. Federal agencies—and to a lesser extent, state and local governments—are powerful economic actors capable of making and shaping markets. Depending on how they steer their spending, governments can impact all three strategic goals of technology and national security policy. Federal contracts and purchasing agreements can incentivize firms to innovate; the U.S. semiconductor industry largely developed in response to the DOD's demand for chips.[38] Procurement bans can undercut powerful foreign firms and reserve a major market segment for companies based in the U.S. or allied countries.[39] We saw Congress employ this instrument in Section 889 of the 2019 National Defense Authorization Act, which prohibited federal agencies from using or working with vendors that use equipment from Huawei, ZTE, and three other Chinese companies. The U.S. government's "Buy American" requirements can have a similar effect in some cases. Procurement requirements can also promote the adoption of new safety and regulatory standards.

Statutes, Regulations, and Standards

Policymakers can also influence the trajectory of technological development through *statutes, regulations, and standards*, or legal rules that govern products, systems, individuals, businesses, and other entities. This lever of power encompasses a broad range of policy instruments, including consumer safety laws, environmental regulations, governance frameworks, insurance schemes, voluntary standards regimes, and legal

rights. Generally, *statutes* are laws created by legislative bodies like Congress to pursue a particular end, *regulations* are detailed instructions for enforcing those laws, and *standards* are specifications for evaluating particular products and services.[40] While statutes, regulations, and standards can take a variety of forms, they typically seek to promote or prohibit certain behaviors, features, or outcomes, either directly or indirectly.

In the technology and national security sphere, statutes, regulations, and standards align most closely with the goal of promoting safe, values-driven deployment. By prohibiting or mandating particular actions, statutes, regulations, and standards can steer technologies and their developers toward socially desirable outcomes. In September 2022, for instance, the Federal Aviation Administration (FAA) published interim safety standards for designing "vertiports," the facilities that will serve as takeoff and landing sites for drones and other aircraft in urban areas.[41] Though urban air mobility is still in its infancy, these regulations will shape the development of the infrastructure that supports those operations. In many cases, however, determining the actions that produce socially desirable outcomes can prove challenging.[42] By locking in certain behaviors and designs, statutes, regulations, and standards can potentially circumscribe certain types of innovation that may ultimately produce more desirable outcomes.

Taxes and Trade

Taxes and trade are another lever of power through which governments can shape the technology and national security landscape. Policymakers frequently rely on tax codes to nudge people, businesses, and other entities toward certain types of behavior; organizations tend to engage in activities that lower their taxes and forgo those that raise their taxes. In the context of technology, taxes have most often been used to promote certain types of technological innovation. For instance, the CHIPS and Science Act included a 25 percent tax credit for capital expenses related to semiconductor manufacturing.[43] The tax code also provides companies with a variety of R&D tax credits, which offset firms' research spending by reducing their tax bill. Taxes have also been used to promote the adoption of certain technologies; the Inflation Reduction Act, for instance, offers up to a $7,500 in tax credit to individuals who purchase qualifying electric vehicles.[44] It is easy to imagine similar tax provisions that incentivize the adoption of certain technologies on the basis of safety and their contribution to popular sovereignty, rights and freedom protection, transparency, and accountability in deliberative processes.

Trade policy is also becoming an increasingly critical component of the country's technology and national security strategy. Tariffs, antidumping duties, import quotas, and other instruments of trade policy can all be structured in ways that impede adversaries' progress by limiting the presence of foreign firms in domestic markets. Such provisions also benefit domestic firms by shielding them from foreign competition, potentially enabling homegrown firms to grow and innovate. However, if domestic firms cannot produce enough supply at the right price, these protectionist policies can limit technology adoption. In June 2022, for instance, the Biden administration temporarily suspended anti-dumping duties on solar panels imported from Cambodia, Malaysia, Thailand, and Vietnam in an effort to avoid postponing high-priority solar energy projects within the United States, against the wishes of domestic equipment producers.[45]

Workforce Development

Policymakers can also pursue different technology and national security policy goals through *workforce development*, a broad lever of power that encompasses efforts to improve the knowledge, skills, educational opportunities, career prospects, and economic outcomes of U.S. workers. Like immigration policies, workforce development efforts generally aim to strengthen the U.S. labor market and talent pipeline, but unlike immigration policies, they focus on enriching the existing domestic workforce rather than expanding it with foreign workers. There are numerous policy instruments that fall in this bucket, including but not limited to education policy, scholarships, training programs, civil rights laws, labor laws, and minimum wage laws.[46] Unlike many other levers of power, workforce development efforts—particularly those related to education—are often left to the jurisdiction of state and local governments rather than the federal policymakers. This decentralization creates an environment in which experimentation is relatively easy but scaling success is often difficult.

In the context of technology and national security, workforce development efforts are often most aligned with the goal of driving technological innovation. Instilling U.S. workers with new knowledge and skills helps them develop new ideas, while \improving career prospects and economic opportunities offers workers the freedom and flexibility to pursue those ideas to their full potential. One notable federal workforce development initiative is CyberCorps, which offers scholarships for cybersecurity-related degree programs in exchange for a period of government service.[47] This program offers participants an opportunity to build their technical skills while also bolstering the government's cyber workforce. Workforce development initiatives can also help promote safe deployment of new technologies. Technologies often reflect the

beliefs and biases of their creators, and creating opportunities for a more diverse set of technologists helps ensure tools are developed and deployed with a wide range of users in mind. Furthermore, education is essential to promoting civic engagement, supporting healthy public discourse, and preserving democratic institutions.

Enabling Levers of Power

The government also has at its disposal different enabling levers of power, which can be used to increase the efficacy of its direct levers. These enabling levers fall into two categories: amplifier levers, which enhance the effect of direct levers; and planning and monitoring levers, which enable policymakers to apply direct levers in more targeted, informed ways. Table 2 provides an overview of these enabling levers.

Table 2. Enabling Government Levers of Power

Lever	Type	Examples
International Coalitions	Amplifier	Formal alliances, informal coalitions
Place-Based Policies	Amplifier	Innovation hubs, regional economic incentives
Information Sharing	Amplifier	Data repositories, agreements
Convening	Amplifier	Summits, strategic dialogues
Research, Analysis, and Intelligence	Planning & Monitoring	Data collection, benchmarking, modeling
Portfolio Management and Bundling	Planning & Monitoring	Diversification strategies

International Coalitions (Amplifier)

In the context of national security, one of the most important enabling levers of power is *international coalitions*. By working with allies and partners, governments can amplify the intended effects of particular policy instruments across the international community. These groupings can be formal, such as alliances, or informal. We have seen both types of coalitions form around export control regimes, for instance. The Wassenaar Arrangement, which controls international trade in conventional weapons and dual-use technology, operates through a formal agreement made between 42 countries in 1996.[48] By contrast, the multilateral economic controls placed on Russia after its full-scale invasion of Ukraine were organized through an informal but coordinated effort between dozens of countries.[49] Were the United States to act unilaterally in either situation, the control regime would likely be much less effective.

Place-Based Programs (Amplifier)

Just as coalitions can enhance policies on the international level, *place-based programs* can amplify levers of power at the local level. Different regions offer unique opportunities and face distinctive challenges, and catering policies to those local idiosyncrasies can amplify their effect both within the region and beyond.[50] In the context of technology and national security, place-based programs can galvanize innovation, economic growth, and workforce development in regions that are underrepresented in other national programs. For example, the Regional Innovation Engines program, launched by the NSF in 2022, targets funding and other resources to areas that "do not have well-established innovation ecosystems."[51] This effort aims to drive technological innovation broadly while also bringing new opportunities to workers, businesses, and researchers in those areas. This development can reduce socioeconomic inequalities that lead to social and political unrest.

Historically, place-based policies have supported the growth of "innovation districts" across the United States. Major tech hubs such as Silicon Valley, Seattle, Austin, Boston, and North Carolina's Research Triangle Park came to prominence partly as a result of government infrastructure investments, workforce development programs, regulatory schemes, and tax benefits.[52] When used in tandem, these policy levers help attract businesses and technical talent into relatively small geographical areas, resulting in high concentrations of capital and knowledge that tend to promote innovation.[53]

Information Sharing (Amplifier)

Information sharing is yet another lever of power that policymakers have at their disposal to amplify the effects of other policies. The government retains vast repositories of information on the global economy, geopolitical landscape, environment, and numerous other systems. Sharing this information with researchers, allies, and other groups can promote collective action and better-informed decisions by actors in any given scenario.[54] In the months before Russia's full-scale invasion of Ukraine, the United States released classified intelligence on Russia's military buildup, which played a critical role in building the coalition that came to Ukraine's aid.[55] These intelligence-sharing efforts have continued throughout the war, playing a critical role in Ukraine's efforts to push back Russian forces.[56] More subtle examples of government information sharing include Data.gov, a public repository of more than 250,000 government datasets that can be used to inform research on education, law enforcement, the economy, climate, and numerous other topics. Policymakers can also derive helpful insights from data collected and aggregated outside the government. Partnering with businesses and other private organizations will be vital to developing effective information programs in the years ahead.

Convening (Amplifier)

Another lever the government can exercise to pursue technology and national security goals is its *convening* power. This general-purpose lever refers to efforts to bring together different actors to address problems, share knowledge, and coordinate collective action. While numerous public and private organizations have convening power, perhaps no other entity can more effectively compel influential individuals, companies, and organizations to mobilize around particular issues than the federal government. Convening relevant individuals and organizations can promote action in virtually any realm of policy. In 2022, the U.S. government convened the first strategic dialogue between the United States and the World Health Organization (WHO), creating a platform for addressing public health issues.[57] The White House has also convened summits around a variety of domestic policy issues, including promoting manufacturing, preserving democracy, and strengthening the cybersecurity workforce.[58]

Research, Analysis, and Intelligence (Planning & Monitoring)

Another crucial general-purpose lever of power in policymakers' toolkit is *research, analysis, and intelligence*. This broad category encompasses a variety of activities

intended to characterize the current state of the world and inform policymakers on how to proceed. Through data collection, benchmarking, modeling, structured analytic methods, and other processes, policymakers can monitor trends in the technology and national security landscape, identify the factors driving those changes, and respond accordingly. Armed with that knowledge, policymakers can determine what levers of power to exercise and when to change course. This feedback mechanism is a critical feature of systems-oriented policymaking.

Establishing a monitoring capability for each policy lever within a broader system should be standard practice; without it, leaders are blind to the outcomes of their own decisions. Today, however, the existing infrastructure is limited to assessments of foreign threats (e.g., intelligence community) or narrowly focused analyses conducted by individual agencies and government-adjacent organizations (e.g., RAND Corporation, the Pew Research Center, the Center for Strategic and International Studies (CSIS)). However, individual organizations are often not incentivized to look at system-wide considerations that are outside of their authority or remit.

Portfolio Management and Bundling (Planning & Monitoring)

Another underappreciated but critical enabling lever of power is *portfolio management and bundling*. In the context of national security and technology, this lever encompasses efforts to diversify government investments, policies, and other programs with the intention of mitigating the impacts of risk. If policymakers lean too heavily on particular programs or strategies in their pursuit of strategic technology and national security goals, they leave themselves and the country vulnerable to major disruptions should that component fail. As with financial portfolios, diversified government strategies are more resilient in the face of disruptions and deliver more reliable long-term outcomes. This approach is implemented both formally and informally at research agencies—which diversify portfolios across fields, applications, and time horizons—and other organizations across government. The professionalization and systematic formalization of this approach may make this policy lever a more formidable option in the future.

Other Options

Federal, state, and local governments within the United States likely have a large number of other levers of power that should be considered. These include law enforcement, kinetic force, covert action, and other tools of hard and soft power. Hard

power levers are typically only pulled when all the others have failed, which underscores the importance of using the other levers effectively.

Conclusion

Navigating the rapidly evolving technology and national security landscape requires a clear vision for the future and a deep understanding of how the government can use different levers of power to realize that vision. Today's fragmented approach to policymaking can obstruct this effort, making it difficult to design holistic strategies and resulting in decisions that fail to recognize the complexity of the problems at hand. A more systems-oriented approach to policymaking—which recognizes the tensions between strategic goals and the differential impact of government policy levers—will enable leaders to chart a more measured, successful course for their country.

This brief aims to provide a framework for this more systems-oriented technology and national security strategy, identifying three strategic technology and national security goals, discussing the inherent tensions between them, and describing 15 levers of power through which policymakers can pursue these goals. There are likely other strategic goals and levers of power that we did not discuss or consider. Nevertheless, we believe this framework is useful for illustrating the complexities of the technology and national security landscape, characterizing government actions, and aligning them to particular goals. Better understanding the government's levers of power can enable more creativity when addressing novel challenges.

However, designing effective technology and national security strategies will require more than frameworks. More comprehensive analysis of individual policy levers and their interactions with one another is essential for constructing a more coordinated, harmonized approach to pursuing strategic goals. Similarly, investing in efforts to monitor the domestic and international national security and economic landscape is vital for understanding the real-time impacts of government policy levers. Armed with this knowledge, leaders can better fine-tune and adapt policies to achieve strategic goals in a rapidly changing world.

Ultimately, successful policy implementation is a challenging endeavor that demands careful thinking, an acute awareness of the political realities, and creative problem-solving. There are no shortcuts to crafting a sound and effective technology and national security strategy. Approaching this process in a more holistic, systems-oriented way will enable leaders to simultaneously pursue and balance the tensions between driving technological innovation, impeding competitors' progress, and promoting safe, values-driven deployment.

Authors

Jack Corrigan is a research analyst at CSET. Melissa Flagg is a Senior Advisor at CSET. Dewey Murdick is CSET's executive director.

Acknowledgements

For feedback and assistance, the authors would like to thank Jacob Feldgoise, Drew Lohn, Evan Burke, Emily Weinstein, Rita Konaev, Igor Mikolic-Torreira, John Bansemer, Helen Toner, Steph Batalis, Jason Ly, William Hynes, Cat Aiken, Micah Musser, Owen Daniels, Bhavya Lal, and Jason Matheny.

Document Identifier: doi: 10.51593/20230018

Endnotes

[1] Gabriela Ramos and William Hynes, *Systemic Thinking for Policy Making—The Potential of Systems Analysis for Addressing Global Policy Challenges in the 21st Century*, Organisation for Economic Co-operation and Development, September 2019, https://www.oecd.org/naec/averting-systemic-collapse/SG-NAEC(2019)4_IIASA-OECD_Systems_Thinking_Report.pdf.

[2] Glen Hepburn, *Alternatives to Traditional Regulation*, Organisation for Economic Co-operation and Development, https://www.oecd.org/gov/regulatory-policy/42245468.pdf.

[3] Michael E. Porter, "What Is Strategy?" *Harvard Business Review*, November 1996, https://hbr.org/1996/11/what-is-strategy.

[4] Chips and Science Act, H.R. 4346, 117th Cong. (2022).

[5] Brendan Thomas-Noone, "What the Cold War can teach Washington about Chinese tech tensions," Brookings, January 12, 2021, https://www.brookings.edu/techstream/what-the-cold-war-can-teach-washington-about-chinese-tech-tensions/.

[6] Shahid Alam, "Restructuring the United States' Export Control Legislation for the Post-Cold War Era," *The Fletcher Forum of World Affairs* vol. 18, no. 2 (1994): 137-149.

[7] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Office of the Director of National Intelligence, February 2023), 6-11, https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf; Office of the United States Trade Representative, *Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, (Washington, D.C.: Executive Office of the President, March 2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[8] Martijn Rasser and Kevin Wolf, "The Right Time for Chip Export Controls," *Lawfare*, December 13, 2022, https://www.lawfareblog.com/right-time-chip-export-controls; Shortly before announcing the Chinese chip controls, National Security Advisor Jake Sullivan called for a fundamental shift in U.S. approach to technology competition. In regards to "foundational technologies" like semiconductors, he said, it is no longer sufficient for the United States "to stay only a couple generations ahead," but instead, "we must maintain as large of a lead as possible." In other words, policymakers should seek to kneecap the progress of U.S. adversaries in strategic technology fields to the greatest extent possible.

[9] Edward Graham, "FCC Bans Sale of New Devices From Chinese Companies Huawei, ZTE and Others," *Nextgov*, November 28, 2022, https://www.nextgov.com/emerging-tech/2022/11/fcc-bans-sale-new-devices-chinese-companies-huawei-zte-and-others/380214/; Jack Corrigan, Sergio Fontanez, and Michael Kratsios, *Banned in D.C.: Examining Government Approaches to Foreign Technology Threats*

(Center for Security and Emerging Technology, October 2022), https://cset.georgetown.edu/wp-content/uploads/CSET-Banned-in-D.C..pdf.

[10] Tim Hwang and Emily S. Weinstein, "Decoupling in Strategic Technologies From Satellites to Artificial Intelligence," (Center for Security and Emerging Technology, July 2022), https://cset.georgetown.edu/publication/decoupling-in-strategic-technologies/.

[11] Antonia Hmaidi and Rebecca Arcesati, "Why Europe Struggles with US Export Controls on China," *The Diplomat*, December 27, 2022, https://thediplomat.com/2022/12/why-europe-struggles-with-us-export-controls-on-china/.

[12] "Pure Food and Drug Movement," *Encyclopedia.com*, accessed March 2023, https://www.encyclopedia.com/history/dictionaries-thesauruses-pictures-and-press-releases/pure-food-and-drug-movement.

[13] Cary Coglianese and Shana Starobin, "Management-Based Regulation" (University of Pennsylvania Carey Law School, 2020), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3228&context=faculty_scholarship#page=3.

[14] Kathleen Curlee and Emmy Probasco, "Comparing Policies and Principles on Trustworthy AI," (Center for Security and Emerging Technology, forthcoming); *Recommendation of the Council on Artificial Intelligence*, (Organisation for Economic Co-Operation and Development, May 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#mainText; *Recommendation on the Ethics of Artificial Intelligence* (United Nations Educational, Scientific, and Cultural Organization, 2022), https://unesdoc.unesco.org/ark:/48223/pf0000381137.

[15] Ramos and Hynes, *Systemic Thinking for Policy Making—The Potential of Systems Analysis for Addressing Global Policy Challenges in the 21st Century.*

[16] European Commission, *A Notification under Article 12 of Regulation (EU) No 1025/2012* (Brussels: Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, May 2022), https://ec.europa.eu/docsroom/documents/52376/attachments/1/translations/en/renditions/native.

[17] Hadrien Pouget, "The EU's AI Act Is Barreling Toward AI Standards That Do Not Exist," *Lawfare*, January 12, 2023, https://www.lawfareblog.com/eus-ai-act-barreling-toward-ai-standards-do-not-exist.

[18] DoD Responsible AI Working Council, *U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway* (Washington, DC: U.S. Department of Defense, May 2021), https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF; Bureau of Arms Control, Verification and Compliance, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*

(Washington, DC: U.S. Department of State, February 2023), https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/; Defense Innovation Board, *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense* (Washington, DC: U.S. Department of Defense, 2019), https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

[19] Tate Ryan-Mosley, "The new lawsuit that shows facial recognition is officially a civil rights issue," *MIT Technology Review*, April 14, 2021, https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/.

[20] National Artificial Intelligence Research Resource Task Force, *Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem: An Implementation Plan for a National Artificial Intelligence Research Resource*, (Washington, DC: Executive Office of the President, January 2023): https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf; "NSF Announces Seven New National Artificial Intelligence Research Institutes," *National Science Foundation,* May 4, 2023, https://www.nsf.gov/cise/ai.jsp; "AI Next Campaign (Archived)," *Defense Advanced Research Projects Agency*, accessed March 2023, https://www.darpa.mil/work-with-us/ai-next-campaign.

[21] Before developing technical standards for responsible AI, the EU was also an early adopter of data privacy regulations. For more, see "Complete guide to GDPR compliance," European Commission, accessed March 2023, https://gdpr.eu/.

[22] Katrina Manson, "The Satellite Hack Everyone Is Finally Talking About," *Bloomberg*, March 1, 2023, https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/.

[23] National Institute of Standards and Technology, *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* (Washington, DC: U.S. Department of Commerce, February 2022), https://csrc.nist.gov/publications/detail/white-paper/2022/02/04/criteria-for-cybersecurity-labeling-for-consumer-iot-products/final; Ryan Daws, "UK, Canada, and Singapore join forces to secure IoT devices," *IoTNews.com*, November 10, 2022, https://www.iottechnews.com/news/2022/nov/10/uk-canada-and-singapore-join-forces-secure-iot-devices/.

[24] *Fact Sheet: U.S.-China Science and Technology Cooperation Highlights: 32 Years of Collaboration* (Washington, DC: Executive Office of the President), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/st-fact-sheet.pdf.

[25] Philippe Aghion, Nicholas Bloom, Richard Blundell, Rachel Griffith, and Peter Howitt, "Competition and Innovation: An Inverted-U Relationship" (NBER, October 2002), https://www.nber.org/system/files/working_papers/w9269/w9269.pdf.

[26] Martin Watzinger, Thomas A. Fackler, Markus Nagler, Monika Schnitzer, "How Antitrust Enforcement Can Spur Innovation: Bell Labs and the 1956 Consent Decree," *American Economic Journal: Economic Policy* 12, no. 4 (November 2020), 328–359.

[27] Daniel A. Crane, "The Tempting of Antitrust: Robert Bork and the Goals of Antitrust Policy" (University of Michigan Law School, 2014), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2549&context=articles; "Art of the Possible: U.S. Chamber International IP Index" (U.S. Chamber of Commerce, 2020), https://www.theglobalipcenter.com/wp-content/uploads/2020/02/GIPC_IP_Index_2020_FullReport.pdf; Exec. Order No. 14036, 86 FR 36987 (2021).

[28] Nicholas Mulder, "The Collateral Damage of a Long Economic War," *Foreign Affairs*, September 26, 2022, https://www.foreignaffairs.com/russian-federation/collateral-damage-long-economic-war.

[29] Emily Kilcrease, "How to Win Friends and Choke China's Chip Supply," *War on the Rocks*, January 6, 2023, https://warontherocks.com/2023/01/how-to-win-friends-and-choke-chinas-chip-supply/.

[30] Hmaidi and Arcesati, "Why Europe Struggles with US Export Controls on China."

[31] Eleanor Olcott and Qianer Liu, "Chinese AI groups use cloud services to evade US chip export controls," *Financial Times*, March 8, 2023, https://www.ft.com/content/9706c917-6440-4fa9-b588-b18fbc1503b9; "Maximum Pressure," (Human Rights Watch, October 2019), https://www.hrw.org/report/2019/10/29/maximum-pressure/us-economic-sanctions-harm-iranians-right-health.

[32] Mark Boroush and Ledia Guci, "Recent Trends in U.S. R&D Performance," *National Science Foundation*, April 28, 2022, https://ncses.nsf.gov/pubs/nsb20225/recent-trends-in-u-s-r-d-performance; Melissa Flagg and Paul Harris, "System Re-Engineering" (Center for Security and Emerging Technology, September 2020), https://cset.georgetown.edu/publication/system-re-engineering/.

[33] National Institute of Standards and Technology, *Notice of Funding Opportunity: CHIPS Incentives Program—Commercial Fabrication Facilities* (Washington, DC: U.S. Department of Commerce, 2023), https://www.nist.gov/system/files/documents/2023/02/28/CHIPS-Commercial_Fabrication_Facilities_NOFO_0.pdf.

[34] David Shepardson, "Biden to require chips companies winning subsidies to share excess profits," Reuters, March 1, 2023, https://www.reuters.com/technology/us-require-companies-winning-chipmaking-subsidies-share-excess-profits-2023-02-28/.

[35] Zachary Arnold, Roxanne Heston, Remco Zwetsloot, and Tina Huang, "Immigration Policy and the U.S. AI Sector" (Center for Security and Emerging Technology, September 2019), https://cset.georgetown.edu/publication/immigration-policy-and-the-u-s-ai-sector/.

[36] "Optional Practical Training (OPT) for F-1 Students," *U.S. Citizenship and Immigration Services,* accessed March 2023, https://www.uscis.gov/working-in-the-united-states/students-and-exchange-visitors/optional-practical-training-opt-for-f-1-students.

[37] Christopher Ali, "The Legacy of the Rural Electrification Act and the Promise of Rural Broadband," *The Law and Political Economy Project*, July 12, 2021, https://lpeproject.org/blog/the-legacy-of-the-rural-electrification-act-and-the-promise-of-rural-broadband/.

[38] Alex Williams and Hassan Khan, "A Brief History of Semiconductors: How the US Cut Costs and Lost the Leading Edge," Employ America, March 20, 2021, https://employamerica.medium.com/a-brief-history-of-semiconductors-how-the-us-cut-costs-and-lost-the-leading-edge-c21b96707cd2.

[39] Corrigan et al., "Banned in D.C."

[40] Regulations and standards can take a variety of forms, as discussed in prior sections.

[41] Federal Aviation Administration, *Engineering Brief No. 105, Vertiport Design* (Washington, DC: U.S. Department of Transportation, September 2022), https://www.faa.gov/sites/faa.gov/files/eb-105-vertiports.pdf.

[42] Pouget, "The EU's AI Act Is Barreling Toward AI Standards That Do Not Exist."

[43] *Fact Sheet: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China* (Washington, DC: Executive Office of the President, August 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.

[44] "Credits for New Clean Vehicles Purchased in 2023 or After", U.S. Internal Revenue Service, April 17, 2023, https://www.irs.gov/credits-deductions/credits-for-new-clean-vehicles-purchased-in-2023-or-after.

[45] Rob Garver, "Biden Drops Tariffs on Southeast Asian Solar Panels for 2 Years," *Voice of America News*, June 7, 2022, https://www.voanews.com/a/biden-drops-tariffs-on-southeast-asian-solar-panels-for-2-years-/6606330.html.

[46] Diana Gehlhaus, Luke Koslosky, Kayla Goode, and Claire Perkins, "U.S. AI Workforce: Policy Recommendations" (Center for Security and Emerging Technology, October 2021), https://cset.georgetown.edu/publication/u-s-ai-workforce-policy-recommendations/.

[47] "Cybersecurity Scholarships," National Institute for Cybersecurity Careers and Studies, accessed April 2023, https://niccs.cisa.gov/education-training/cybersecurity-scholarships.

[48] "The Wassenaar Arrangement at a Glance," Arms Control Association, February 2022, https://www.armscontrol.org/factsheets/wassenaar.

[49] Chad P. Brown, "Russia's war on Ukraine: A sanctions timeline," *Peterson Institute for International Economics*, May 8, 2023, https://www.piie.com/blogs/realtime-economics/russias-war-ukraine-sanctions-timeline.

[50] Rana Foroohar, "After Neoliberalism: All Economics Is Local," *Foreign Policy*, October 28, 2022, https://www.foreignaffairs.com/united-states/after-neoliberalism-all-economics-is-local-rana-foroohar.

[51] "Regional Innovation Engines," National Science Foundation, accessed April 2023, https://new.nsf.gov/funding/initiatives/regional-innovation-engines.

[52] Bruce Katz and Julie Wagner, "The Rise of Innovation Districts" (Metropolitan Policy Program at Brookings, May 2014), https://c24215cec6c97b637db6-9c0895f07c3474f6636f95b6bf3db172.ssl.cf1.rackcdn.com/content/metro-innovation-districts/~/media/programs/metro/images/innovation/innovationdistricts1.pdf.

[53] Diana Gehlhaus, James Ryseff, and Jack Corrigan, "The Race for U.S. Technical Talent," (Center for Security and Emerging Technology, forthcoming).

[54] Hepburn, "Alternatives to Traditional Regulation."

[55] Julian E. Barnes and Adam Entous, "How the U.S. Adopted a New Intelligence Playbook to Expose Russia's War Plans," *The New York Times*, February 23, 2023, https://www.nytimes.com/2023/02/23/us/politics/intelligence-russia-us-ukraine-china.html.

[56] Julian E. Barnes and Helene Cooper, "Ukrainian Officials Drew on U.S. Intelligence to Plan Counteroffensive," *The New York Times*, September 10, 2022, https://www.nytimes.com/2022/09/10/us/politics/ukraine-military-intelligence.html.

[57] "Joint statement of the United States of America and the World Health Organization on the U.S.-WHO strategic dialogue," World Health Organization, September 27, 2022,

https://www.who.int/news/item/27-09-2022-joint-statement-of-the-united-states-of-america-and-the-world-health-organization-on-the-u.s.-who-strategic-dialogue.

[58] *Readout of the First White House Leadership Summit with Manufacturing USA Innovation Institute Network Directors* (Washington, DC: Executive Office of the President, October 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/24/readout-of-the-first-white-house-leadership-summit-with-manufacturing-usa-innovation-institute-network-directors/; "Summit for Democracy 2023," U.S. Department of State, accessed April 2023, https://www.state.gov/summit-for-democracy-2023/; *FACT SHEET: National Cyber Workforce and Education Summit* (Washington, DC: Executive Office of the President, July 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/21/fact-sheet-national-cyber-workforce-and-education-summit/.