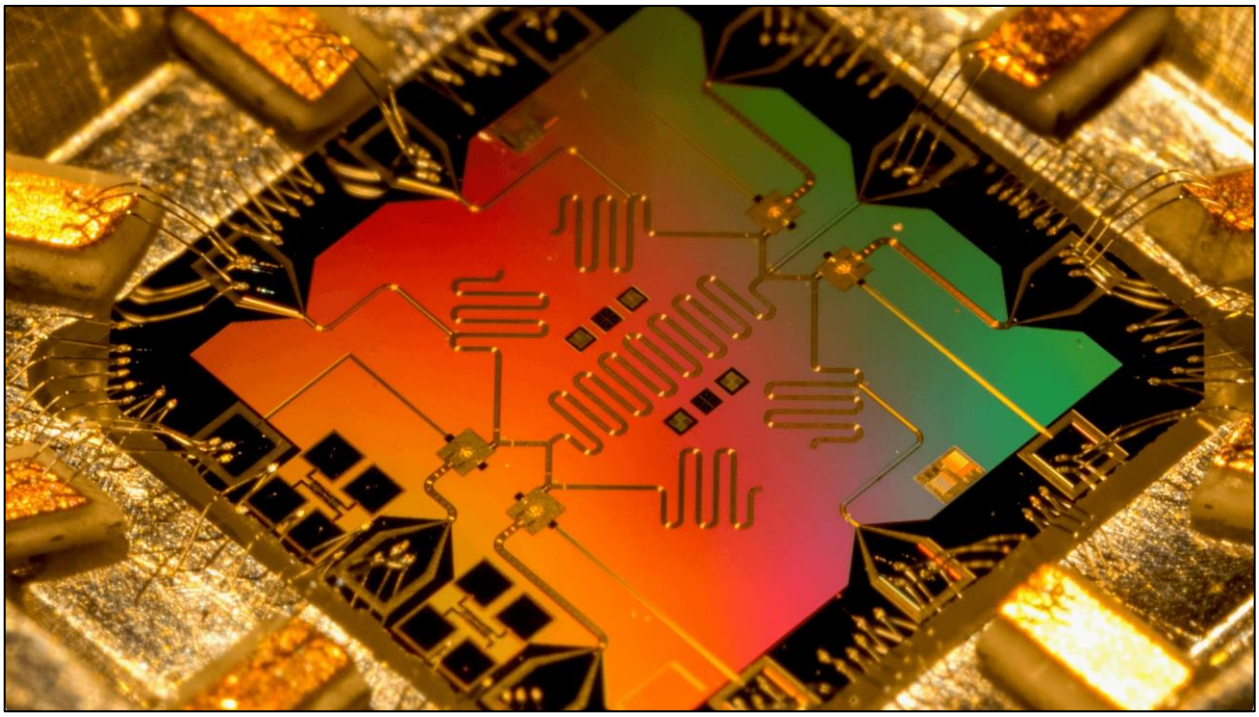
The Desirability and Feasibility of Strategic Trade Controls on Emerging Technologies

A CISSM Report | June 2023



Nancy W. Gallagher, Lindsay Rand, Devin Entrikin, & Naoko Aoki

SCHOOL OF PUBLIC POLICY
CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

Executive Summary

Artificial intelligence (AI), quantum computing, robotics, hypersonics, and other rapidly developing technologies have many beneficial civilian and military uses. They also raise a range of serious security concerns, including hostile use by a peer competitor, proliferator, or terrorist organization. Moreover, irresponsible behavior by the many countries, companies, academic researchers, and ordinary citizens around the world who now have access to cutting-edge technologies could accidentally kill millions of people, cause a global financial collapse, or even trigger some disastrous outcome that seems like science fiction today.

Policymakers must decide whether and how to regulate the development, sale, and use of emerging technologies so the security benefits outweigh the economic, technological, and political costs. They have faced that question before, so lessons can be learned from historical experience. It has never been easy to get agreement about what types of governance mechanisms are most desirable, or to implement those controls effectively enough to achieve the security objectives. Many different approaches have been tried but only some legacy arrangements could be applied to emerging technologies, while others would do more harm than good.

Four features make the current iteration of the dual-use problem particularly challenging. (1) Emerging technologies are largely intangible rather than physical. (2) The private sector is now the main engine for innovation, often independent from and resistant to government control. (3) Concerns about dual-use emerging technologies expand beyond their relevance to weapons of mass destruction (WMD) to their much broader utility for conventional warfighting. (4) Political and economic relations among the countries at the forefront of technology innovation are also very complex and uncertain, further complicating efforts to get agreement about what greatest security risks are, and what mix of competition and cooperation offers the most cost-effective way to reduce them.

To help policymakers and other stakeholders assess what governance mechanisms are feasible for various types of emerging technologies, and which of those options could get enough support from all the relevant parties to produce the desired security benefits, this report identifies four approaches used in the past and applicable to current challenges. Three of them try to deny dangerous states and nonstate actors' critical information, material, technology, and products that could increase their destructive capabilities, while the fourth is a more cooperative demand-side strategy. The approaches are:

- *Unilateral access denial* seeks to maintain U.S. technological monopolies across global markets or in direct relations with peer competitors with diverging security agendas.
- *Allies versus adversaries* uses technology transfers to build up the military and economic power of countries aligned with the United States relative to potential adversaries.
- *Suppliers against seekers* coordinates decision-making among those that have dangerous dual-use technologies about what is safe to sell and what should be withheld from countries of concern or specific entities within those countries.

- *Cooperative management* facilitates trade and indigenous development of powerful dual-use technologies subject to consensual agreements among all relevant stakeholders on rules for acceptable use and safeguards or other transparency arrangements to document compliance and facilitate detection of illicit activities.

A historical review of efforts to control dangerous dual-use technologies during and after the Cold War shows that all four approaches have been used for different purposes at different points in time. Which approach was chosen and how well it worked depended on four factors:

- the global security and economic context,
- the characteristics of the technology in question,
- the current state of technological development and distribution, and
- the relevant stakeholders' interests and ideas about managing dual-use technology.

During the Cold War, the main objective of U.S. export control policy was to maximize how much military, economic, and technological power the United States and its allies had compared to the Soviet Union and other communist countries. *Unilateral access denial* and *allies versus adversaries'* approaches were used to regulate trade related to advanced conventional military capabilities, with limited success and uneven stakeholder support, causing much frustration and fluctuation over time. Despite intense bilateral nuclear competition, the two superpowers worked together to slow the spread of nuclear weapons, especially to their own allies. The *cooperative management* methods developed in the nuclear sphere were weaker than some would have liked, but more stable and successful than denial-based controls on conventional technologies.

Post-cold war efforts to slow proliferation of WMD show a similar pattern of *cooperative management* methods being weaker, but more successful and sustainable than denial-based approaches. *Cooperative management* arrangements applied to chemical, biological, and space/missile technologies have evolved slowly, but provide enough security benefits to outweigh relatively low economic, technological, and political costs. They have been supplemented with *unilateral* and *suppliers against seekers* restraints. These denial-based efforts have slowed but rarely stopped acquisition of dual-use capabilities by determined proliferators. They have also spurred indigenous technology development; raised questions about compliance, including by some U.S. administrations; and sparked domestic political opposition.

The benefit/cost calculation for current strategic trade control options depends on what the dominant security concern is. The Obama administration remained primarily focused on WMD proliferation as some security experts sounded alarms that major technological advances by China and Russia were eroding U.S. military advantages. The Trump administration emphasized renewed great power competition while trying and failing to use strategic controls and sanctions to pressure Iran and North Korea into making nuclear concessions.

The Biden administration's National Security Strategy (NSS) centers around "responsible" competition between democratic and autocratic powers, combined with transactional cooperation

with China and Russia to address shared global challenges like WMD proliferation.[1] In today's great power competition, the "pacing threat" comes from China – a country with whom the United States and its allies are much more economically interdependent than they were with the Soviet Union, and one that is a peer economic and technological rival, not just the military equal to the United States. Little attention has been paid to how making China and Russia the primary targets of U.S. technology denial efforts will affect prospects for cooperation to enhance strategic stability and slow the spread of emerging technologies to other countries potentially engaged in WMD proliferation.

There is broad bipartisan consensus in principle that strengthened strategic trade controls on critical emerging technologies are desirable ways to ensure U.S. leadership in scientific innovation, cutting-edge military applications, and global markets. In response to legislation passed in 2018, the Commerce Department's Bureau of Industry and Security (BIS) identified fourteen categories of emerging technologies that are candidates for new controls on trade, finance, and investment.[2] The Biden administration's technology policy prioritizes what it considers the three most critical sectors: advanced computing (including microelectronics, quantum information systems, and AI), biotechnology, and clean energy.[3] The first two sectors are on the BIS list, but not the third.

Less attention has been paid to determining what types of measures are feasible – i.e., have a reasonable chance of preventing deliberate and inadvertent misuse by state and nonstate actors without serious practical implementation problems, including capacity, cost, verifiability, and compliance management capabilities. Some export control methods that worked relatively well in the past are less feasible today due to economic interdependence, the global spread of software technologies, and the importance of multinational corporations and other private sector actors.

An even more difficult task is to determine which specific feasible management mechanisms are also desirable in practice– i.e., are likely to reduce security risks without unnecessary negative impacts on military, economic, political, and technical interests. Different stakeholders have divergent interests and ideas that shape their calculations about what governance mechanisms would be cost-effective, as evidenced by recurrent debates about whether export decisions related to commercial satellites and other dual-use items should be handled by the U.S. Commerce Department or the State Department. Different U.S. administrations have also had world views and national security strategies that predisposed them towards more unilateral decision-making and denial-based forms of export controls, or more cooperative arrangements. Another common source of disagreement within the United States and among groups of

[1] Biden-Harris Administration National Security Strategy, October 2022, p. 3, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
[2] Federal Register, Vol. 83, No. 223, Monday, November 19, 2018 (Proposed Rule) Rules https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies
[3] "Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit," September 16, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/

countries working together to control the spread and use of dangerous technologies has been whether the rules should be legally binding, or voluntary principles and best practices.

This report employs a socio-technical evaluation focused on seven considerations that vary widely across different sectors to determine which strategic trade controls would be both feasible and desirable for a specific category or sub-category of emerging technology:

- Technology make-up: Are systems and components hardware or software-based? When there are limited sources of critical raw materials or subcomponents for hardware-based systems, it may be feasible to control flow of physical items through a chokepoint, or critical node in the supply chain. If a technology is almost entirely software-based, efforts to deny access are likely to fail. It may be feasible to implement end-use controls by requiring coding or parameters that preclude operation of a software technology under specific circumstances (e.g., accepting certain types of data from unauthorized end-users), but this remains speculative.

- Technology fabrication process: This dimension includes the design, manufacturing, and testing phases required for developing a given technology. It also encompasses the facilities needed, and the tacit knowledge or human resources required to ultimately develop and operate the technology. The more difficult and expensive it is to acquire the necessary facilities and expertise, the higher the barriers to entry will be and the longer indigenous development will take regardless of material availability.

- Stage of Development and Dispersion: Technologies in early stages of research and development (R&D) are hard to monitor, but easier to control in other regards than when applications have already been widely commercialized. There is more uncertainty early on about what will be technologically feasible, complicating efforts to get multistakeholder agreement on the benefits and costs of controls. The more widely dispersed advanced forms of emerging technologies are, the larger the number of stakeholders who must participate for a control arrangement to be effective.

- Dual-Use Applications: The larger the likely commercial market for civilian applications of emerging technologies, the more likely private sector actors are to invest their own funds in research and product development and to enjoy economies of scale. This reduces costs for military purchases, but also makes it harder to design and implement controls that preclude adversaries from leveraging products purchased on the open market but that do not reduce companies' profits, slow innovation, incentivize illicit sales, and stimulate domestic political opposition to burdensome strategic trade controls.

- Disruption Mechanism: By definition, emerging technologies disrupt established practices in ways that various stakeholders may view as positive, negative, or mixed.

They can affect nuclear deterrence by altering the prospects for a disarming first strike, improving intelligence about potential adversaries' military preparations, blurring offensive/defensive and nuclear/conventional distinctions, and shortening decision-time. They can impact global security by altering regional military balances and helping weaker states or nonstate actors to emulate or offset what stronger countries can do. They also can improve verification, spread disinformation, enhance government surveillance, empower civil society actors, and much more.

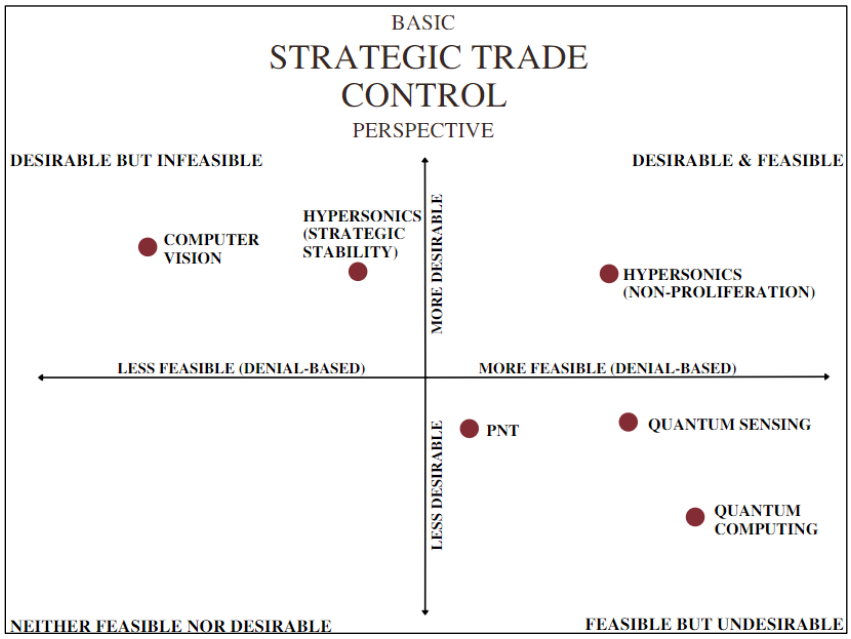
- Stakeholder Community and Power Distribution: Each of the factors above affects what mix of government, private sector, and civil society actors in which different countries count as critical stakeholders for the design and implementation of effective mechanisms to govern emerging technologies. How these players interact depends on various structural factors at the national and international levels, including the distribution of political and economic power; institutional arrangements for developing and implementing technology, trade, and investment controls; cultural norms about state-business interactions; and the current state of international relations.

- Scientific Promise: The current state of scientific knowledge limits how much near-term advancement is realistic. It also informs assessments of the theoretical limits on what the most advanced version of the technology could accomplish. Those assessments may be widely understood, or involve significant uncertainty and debate about what is doable given enough time, money, and ingenuity.

This report illustrates the importance of technology-specific considerations by summarizing key findings from a sectoral mapping exercise conducted for five technologies on the BIS list: position, navigation and timing (PNT) technologies; quantum computing; computer vision; hypersonics; and quantum sensing. From the perspective of a U.S. policymaker charged with determining how strategic trade controls could enhance national security, a sectoral analysis would indicate that denial-based controls are potentially feasible for certain aspects of some technologies studied, but not others. It would also find that controls on emerging technologies with clearly negative disruptive effects would be more desirable than controls on technologies with positive, disputed, or unknown disruptive effects.

The chart below depicts a basic assessment of the desirability and feasibility of denial-based strategic trade controls on the five emerging technologies studied. The quadrants, and positions within each quadrant, that the different technologies occupy are determined based on the sectoral analyses, with the assessment of desirability and feasibility of trade control policies for each technology visualized through their positions along the axes and indicating spectra of negative to positive desirability and feasibility estimations. Although the specific positions for each technology are subjective with respect to the scope of policies considered and the assessment of the technical traits considered, we indicate their locations with the specific scope of trade control policies and based on our assessment of the current state of technical and political

characteristics. Since others may differ in some of their assessments, this type of quad chart can be a useful mechanism for analysts and stakeholders to debate why they think strategic trade controls on these emerging technologies are more or less feasible and desirable than we have indicated.



Given the limited scope of denial-based control approaches, most emerging technologies are filtered out of consideration by feasibility or desirability constraints. As a product of the technologies being selected on the basis that policymakers have identified them either as being feasible to control or desirable based on some strategic rationale, no technologies in this study fit in the bottom left quadrant. Conversely, our analysis finds that the only technology that could be both feasibly controlled and for which controls may be strategically desirable among enough key stakeholders is hypersonic technology. The caveat for the hypersonic case is that trade control policies would only be desirable from a non-proliferation perspective, in which limiting the number of countries that could acquire the technology is desirable, regardless of which countries they are.

Instead, most technologies are filtered into either the upper left quadrant (desirable, but not feasible) or the lower right quadrant (feasible, but not desirable). Although some policymakers, private sector actors, or civilians have expressed interest in controls for computer vision or hypersonic technologies, our assessment finds that controls over these technologies would be infeasible due to the high degree of dispersion and intangible components for computer vision technologies and because key actors that are likely to be the target of controls have already acquired the technology in the case of hypersonic technologies. Meanwhile, some emerging technologies like advanced PNT, quantum sensing, and quantum computing could – to some extent – feasibly be controlled for a finite period given current U.S. leadership, restricted access to key materials, and R&D nascency. These technologies, though, generally lack a clear enough security risk that outweighs potential benefits of private sector development to rally key stakeholders around the desirability of trade controls.

Visualizing the problem from this perspective helps explain why progress applying new strategic trade controls to emerging technologies has been, and will remain, very slow despite the broad bipartisan consensus in the United States that tighter controls are urgently needed to widen gaps

in critical technologies that promise major strategic advantages. Denial-based controls are assessed to be both feasible and desirable for only one of the five technologies surveyed—hypersonics – and only if the security objective is nonproliferation. The feasibility assessment reflects the technical characteristics of the sector, but political relations between the three most advanced countries are not currently conducive to a *suppliers against seekers* arrangement. If the security objective is to enhance strategic stability, the Chinese and Russian programs are advanced beyond the point where denial efforts could be very effective. Cooperative arms control and confidence-building measures would be the most cost-effective way to reduce fears of surprise attack, incentives for preemption, and arms racing. Cold war history indicates that such agreements are feasible among potential adversaries *if* they are mutually beneficial and jointly developed.

There are other reasons why this simple schematic should only be used as a starting point for thinking creatively about what types of governance mechanisms can and should be applied to different aspects of emerging technologies. It provides only one type of stakeholder's perspective: that of a U.S. official tasked with using strategic trade controls to enhance national security. Other stakeholders could disagree about where to locate each technology because they make a different benefit/cost calculation or think not only about chokepoints where consequential controls might be feasible in principle, but also about the practicalities of implementing such controls effectively. Placement on the chart also reflects the current state of each technology's development and diffusion; denial-based controls will be less feasible as advanced capabilities spread over time.

The "neither feasible nor desirable" cell is blank because one criterion for selecting technologies to survey was strong current demand for controls (computer vision) or being early enough in the development and diffusion process for chokepoints to still exist. AI is among the emerging technology sectors that the most powerful stakeholders would put in the neither feasible nor desirable cell, but some civil society groups are already calling for controls on certain high-consequence applications, like lethal autonomous vehicles. If a stronger consensus develops about the desirability of rules for responsible use, *cooperative management* would be the most feasible approach. Such a consensus already exists in the United States about the desirability of keeping repressive governments from using computer vision to enhance domestic surveillance. Here, also, a *cooperative management* system centered around data restriction or end-use agreements would probably be more cost-effective than any denial-based strategy for reducing the risks of misuse.

Taken together, the findings of this historical and technical survey contain important lessons for policymakers tasked with trying to manage the spread and use of emerging technologies. First, policymakers need to decide what the primary objective of strategic trade controls is. For most of the post-Cold War period, the priority was to reduce risks from WMD proliferation, but current efforts are primarily concerned with strategic advantage in great power competition. China and Russia have advanced capabilities in some emerging technology sectors. How do the security benefits of using *unilateral* or *allies versus adversaries* approaches to slow those countries' technological progress compare with those *suppliers against seekers* arrangements to control the spread of these capabilities to other dangerous states and nonstate actors?

Second, the historical analysis shows that, even under relatively favorable geopolitical, economic, and technological conditions, any type of denial-based control effort will be a stopgap solution at best and is likely to have unintended negative consequences. The more stringent the controls, the more opposition to them will grow inside the United States, in partner countries that are more sensitive to their costs, and in target countries that resent technological discrimination.

Third, using *cooperative management* as the primary governance approach for WMD-relevant aspects of nuclear, chemical, and biological technologies has had strengths and weaknesses, too. It involves compromises and concessions that the United States is often loath to make, especially when it distrusts some countries whose participation is a prerequisite for success. The current political context in the United States and among major world powers makes it hard to imagine this becoming a viable option again. Yet, the establishment of cooperative controls on nuclear technology during the Cold War shows that when the unregulated spread of powerful dual-use emerging technologies poses a serious threat, and denial-based controls will not work for some reason, innovative forms of cooperative management may gain support.

Fourth, the socio-technological characteristics of critical emerging technology fields indicate that getting multi-stakeholder agreement on denial-based controls will be harder, implementation will be more challenging, and the outcomes will be less stable than they were in the past. Policymakers will need to be extremely selective, focusing not only on the subsets of emerging technology of greatest importance to national security, economic growth, and well-being, but also on specific control options that are both technically feasible and broadly desirable. This poses a particular challenge when the intended targets for control measures are close to or equally technologically advanced, in contrast to nonstate actors or actors with limited technical capabilities, which were the primary focus of export control policies geared at preventing WMD proliferation. Quietly developing cooperative management strategies to minimize the most serious security risks posed by other technologies on the BIS list without restricting trade or slowing technological innovation would be a relatively low-cost way to proceed under difficult circumstances.

Finally, before policymakers can recognize security imperatives to control some aspect of a dual-use emerging technology, and get the necessary multi-stakeholder buy-in, technological advancement and diffusion often cause those arrangements to be outmoded, if not obsolete. This puts a premium on having the right mix of technology and policy expertise to more quickly determine when new controls on dangerous aspects of emerging technologies are needed, and what could be both feasible and cost-effective. Giving policymakers the capacity to evaluate the security implications of technological advances, understand sectoral characteristics well enough to make complex cost-benefit calculations, and adjust quickly to new information involves building up in-house scientific and technical expertise and making analysis from non-governmental experts more accessible and policy-relevant. It also requires strong advocates for cost-effective emerging technology governance arrangements throughout the U.S. government.

U.S. inter-agency debates about how to balance security, economic, technological, and other interests affected by export controls and other technology governance options need to better

understand the interests and concerns of non-governmental and international stakeholders. These partners will contribute more enthusiastically and reliably if they are involved from the start in the design, implementation, and adaptation of governance mechanisms. Even though U.S. policymakers, foreign partners, and private sector players will often have different concerns and interests that make specific governance mechanisms more or less desirable, achieving a baseline level of consensus will improve compliance and efficacy of whatever governance approach is applied to different aspects of emerging technology.

Table of Contents

List of Abbreviations

AI	Artificial Intelligence
ANPRM	Advanced Notice of Proposed Rulemaking
ASAT	Anti-satellite technology
BIS	Bureau of Industry and Security
CCL	Commerce Control List
CFIUS	Committee on Foreign Investment in the United States
COCOM	Coordinating Committee for Multilateral Export Controls
DIUx	Defense Innovation Unit Experimental
DOD	Department of Defense
EAA	Export Administration Act
ECRA	Export Control Reform Act
EXBS	Export Control and Related Border Security Program
FDPR	Foreign direct product rule
FIRRMA	Foreign Investment Risk Review Modernization Act
GAAFET	Transistor structure
GDP	Gross Domestic Product
GPS	Global Positioning System
IAEA	International Atomic Energy Agency
MTCR	Missile Technology Control Regime
NAS	National Academy of Sciences
NATO	North Atlantic Treaty Organization
NPT	Treaty on the Nonproliferation of Nuclear Weapons
NSG	Nuclear Suppliers Group
NSS	National Security Strategy
NWS	Nuclear Weapons State
NNWS	Non-nuclear Weapons State

OST	Office of Science and Technology
PNT	Positioning, navigation, and timing
PRC	People's Republic of China
PSI	Proliferation Security Initiative
PV	Photovoltaic
R&D	Research and development
RMA	Revolution in Military Affairs
START	Strategic Arms Reduction Treaty
STEM	Science, Technology, Engineering, and Math
SWaP-C	Size, weight, power, and cost
UNSCR	United Nations Security Council Resolution
USML	United States Munitions List
USSR	Union of Soviet Socialist Republics
WMD	Weapons of Mass Destruction

Introduction

Policymakers, technologists, and security experts are trying to determine what existing or new governance mechanisms should be applied to emerging technologies to reduce security risks. This is the most recent iteration of a long-standing problem involving rapidly advancing technologies with a wide range of potential civilian benefits and commercial appeal, but also military applications that could provide significant strategic advantages in great power competition, asymmetrical attack options for proliferators, novel opportunities for catastrophic terrorism, and inadvertent dangers from irresponsible management.

The problem has manifested differently during major time periods since World War II, depending on the security and economic context, the technology in question, and the current U.S. administration's views on security, trade, and technology policies. During the Cold War, when the central security problem was superpower rivalry, the United States had economic and technological dominance that declined over time. Differences in technological characteristics and stakeholder composition prompted U.S. policymakers to take very different approaches to dual-use dilemmas related to nuclear technology and to advanced conventional military capabilities. After the Cold War ended and the global economy became much more interconnected, policymakers agreed that the primary security risks were proliferation of and terrorist access to technologies that could be used to make WMD, but they disagreed about what types of strategic trade controls could enhance security without harming economic competitiveness, technological progress, and political relations due to different worldviews and national security strategies. We now appear to be entering a third era where the spotlight on renewed great power competition seems to be overshadowing attention to proliferation and terrorism, and where the commercial sector is driving innovation in AI, space, quantum capabilities, and a range of other digital technologies. The prospect of China overtaking the United States and its European and Asian allies for technological leadership and market dominance in key sectors has generated a bipartisan consensus in the United States on the need in principle for tighter controls on dual-use emerging technologies, but little agreement in practice on what can and should be done.

To inform consideration of that question, we lay out four basic approaches to managing the benefits and risks of emerging technologies that have featured prominently in past U.S. debates. Three approaches rely on secrecy and access denial to keep dangerous capabilities away from U.S. enemies. *Unilateral access denial* seeks to maintain U.S. technological monopolies; *allies versus adversaries* uses technology transfers to build up the military and economic power of countries aligned with the United States relative to potential adversaries; and *suppliers against seekers* coordinates decision-making among those that have dangerous dual-use technologies about what is safe to sell and what should be withheld from countries of concern or specific entities within those countries. The fourth approach, *cooperative management*, facilitates trade and indigenous development of powerful dual-use technologies subject to consensual agreements among all relevant stakeholders on rules for acceptable use and safeguards or other transparency arrangements to document compliance and facilitate detection of illicit activities.

A historical review of U.S. efforts to control dangerous dual-use technologies during and after the Cold War shows that all four of these approaches have been used for different purposes at

different points in time. Which approach was chosen and how well it worked depended on four factors: the current global security and economic context, the characteristics of the technology in question, the current state of technological development and distribution, and the relevant stakeholders' interests and ideas about managing dual-use technology.

The cooperative management methods used in the nuclear sphere are weaker than some would like, yet have been remarkably stable and relatively successful over time. There has been much more frustration and fluctuation over time with mechanisms developed to regulate trade in technologies related to advanced conventional military capabilities. The net result is a patchwork of U.S. regulations, international rules, and cooperative institutions developed for different purposes at different times. Some of them could be helpful for reducing security risks associated with various types of emerging technologies, while others would be impossible to apply effectively, or would impose economic, technological, and political costs that would outweigh whatever security benefits might be achieved.

The most recent major legislative reform of the U.S. export control system and its foreign investment risk review process occurred in 2018. That spurred the Commerce Department to solicit public comments about applying strategic trade controls to certain categories of emerging technologies. Despite bipartisan consensus that the United States should be at the forefront of development in all of these fields, and should do more to prevent China, Russia, and other potential adversaries from using products and knowledge developed in the United States to threaten U.S. interests, socio-technical analysis demonstrates how difficult it will be to get agreement on specific control mechanisms. We examine five types of emerging technology:

- advanced position, navigation, and timing technology
- quantum computing
- computer vision
- hypersonics
- and quantum sensing

This study will illustrate how the technical and social characteristics of each sector impacts the feasibility and desirability of different governance options. Using a socio-technical framework for analysis, we identify different control mechanisms that might be feasible for each of the five technology sectors. Different governmental and non-governmental stakeholders are likely to have divergent views, though, about whether the potential security benefits of those feasible options outweigh potential economic, political, and technological costs. This complicates prospects for agreement on specific controls among all of the stakeholders whose participation is necessary to achieve the desired security benefits.

In previous export control eras, the U.S. government often dealt with divergent preferences by trying to coerce other countries and commercial actors into following stricter export control practices than they desired, but this was difficult and expensive to implement. Unilateral U.S. efforts at coercive export controls were only semi-effective under relatively conducive circumstances, and sometimes backfired by stimulating indigenous technology development. The

conclusion suggests that such high-handed ways of dealing with divergent preferences will be even less effective under current conditions. The United States no longer has the most advanced capabilities across all types of emerging technologies, views global economic competitiveness as a key component of national security, and relies on powerful private sector companies as independent engines of technological innovation. If U.S. policymakers can decide whether the primary objective of strategic trade controls should now be to gain advantage in great power competition or to slow proliferation of WMD-related emerging technologies, they may be able to buy some time by strengthening *allies versus adversaries* or *suppliers against seekers* governance mechanisms, but it would be counterproductive to pursue these contradictory types of denial strategies at the same time. *Cooperative management* seems like the least plausible governance option under current geopolitical conditions. But, as the superpowers came to see for nuclear technology during the Cold War, it may turn out to be the only practical way to reduce the worst security risks from emerging technologies while facilitating global trade, investment, and beneficial applications.

Framework for Analysis

The label "dual-use technology" commonly refers to technologies that have both beneficial and dangerous or malign applications. That phrase is frequently associated with nuclear, chemical, biological, and missile technologies, but the concept is also relevant for Cold War efforts to limit communist countries' ability to access to space, computer, and other technologies related to advanced conventional weapons. Sometimes the line is drawn between peaceful and military uses; other times, certain military uses or military users are considered beneficial, while others are viewed as dangerous. For example, imagery satellites can be used for a wide array of civilian and commercial purposes; or for security-related applications that help reduce the costs and risks of nuclear deterrence, including early warning and arms control verification; or for making weapons targeting more accurate, which may seem beneficial for one's own military and threatening in an adversaries' hands. Some security experts consider any technology with potential future military applications to be dual-use, while many scientists and entrepreneurs who are focused solely on civilian applications reject such hypothetical concerns.[4] With other technologies, such as hypersonics, the military applications are clear while the civilian uses are much less clear and practical, raising questions about whether countries that say they are only interested in peaceful applications actually have military ambitions. Thus, even the most basic definitional questions about whether policymakers should try to facilitate or restrict the development, spread, and use of a given technology involves a complicated mix of technical and socio-political considerations.

Decisions about the governance of dual-use technologies involve balancing benefits and risks. Numerous benefits can be obtained by directly facilitating technology development or creating a regulatory environment that is conducive to research, development, and commercialization by academics and private companies. These include practical benefits provided by goods and services based on that technology, economic benefits from selling those goods and services, and

[4] Elisa Harris, "Introduction," in Governance of Dual-Use Technologies: Theory and Practice, ed. Elisa D. Harris, (Cambridge: American Academy of Arts and Sciences, 2016), 4-7.

socio- political benefits from demonstrating technological mastery, sharing advanced capabilities with other countries, or cooperating with them on technological challenges too complicated or expensive to do on one's own.

There are also various risks associated with dual-use technologies. They could be deliberately (mis-)used by a hostile state or terrorist organization to attack or intimidate the United States, its allies, or other countries. They also can be handled irresponsibly, such as lax biosafety practices leading a dangerous pathogen to leak from a laboratory and inadvertently start a global pandemic. A rival country's breakthrough advances in basic research on emerging technologies and state-of-the-art achievements for purely peaceful goods and services can even be characterized as security threats when a zero-sum view of great power competition leads any technological, economic, or political gain for one side to seem like a dangerous loss of relative power for other players.

Both the technical and the social characteristics of a particular dual-use technology will determine what governance options are feasible – i.e., have a reasonable chance of preventing deliberate and inadvertent misuse by state and nonstate actors without serious practical implementation problems, including capacity, cost, verifiability, and compliance management capabilities. Technical characteristics include what types of systems and components comprise the technology, such as physical versus digital, and whether supplies of raw materials and components are scarce or abundant. Features of the technology fabrication process, such as whether unusual and expensive testing or manufacturing facilities are required, whether workers must have special skills, and how much tacit knowledge is necessary for high-quality production, have implications for the feasibility of different types of control arrangements. The stage of technology development – from nascent discovery through exhaustive understanding, and from basic research through widespread commercialization – also matters. So does whether a single country has a monopoly on the most advanced forms of that technology, a handful of companies and countries have access, or whether the technology is widely available to state and nonstate actors around the world. Social characteristics that influence feasibility include the nature of and relationships among different state and nonstate actors who have a stake in how a given technology is developed and used. This includes whether the most dangerous aspects of a dual-use technology are directly under the control of an international organization, national military officials, or private companies operating under lax or strict oversight from governmental regulators or international safeguards officials.

Different stakeholders involved in policy decisions about governance of dual-use technologies are likely to have different interests and ideas about what, if any, control mechanisms would be desirable – e.g., are likely to reduce security risks without unnecessary negative impacts on military, economic, political, and technical interests. In the United States, stakeholders typically include various parts of the Executive Branch (particularly the President, State Department, Commerce Department, Department of Defense (DOD), and national labs), members of Congress, companies that want to sell dual-use services and products, and academic scientists and engineers. Other countries can be stakeholders in U.S. policy deliberations when they are potential recipients of controlled technologies or suppliers under pressure to follow U.S. export control regulations, and other types of U.S. strategic trade controls, such as restrictions on

exchange of knowledge (deemed exports) and foreign investments in strategic industries and critical infrastructure in the United States. Other countries involved in the negotiation and implementation of multilateral export control arrangements are also stakeholders. While those countries have similar types of internal stakeholder groups, different political systems can have different norms about government-private sector relations, and more top-down or inclusive decision-making processes.

Previous debates about how to manage new types of dual-use technologies highlight dilemmas that deserve careful consideration by those making similar decisions today. They illuminate difficult tradeoffs among policy objectives of security, economic gain, and technological advancement. Alternative types of trade controls also involve tradeoffs. The benefits that might be gained by using secrecy and access control to preserve a monopoly, or a very large lead, in a new and rapidly advancing dual-use technology must be weighed against the potential benefits of sharing information and access with other countries to learn more about what they are doing, and possibly develop better cooperative control mechanisms. Moreover, since economic gains from technology commercialization can be measured in relative terms (market share) or absolute terms (size of the market), trying to maximize one type of economic gains could harm the other. Efforts to protect or regain a U.S. lead in some aspect of technological innovation could hinder the global rate of innovation, while policies that encourage international technological collaboration could speed innovation in ways that benefit other countries as much or more than the United States. They also show that different stakeholders placed varying emphasis on security, economic, and technology innovation objectives, and had divergent views about what strategies would advance their objectives.

Governance mechanisms applied to cutting-edge dual-use technologies during and after the Cold War can be divided into four broad approaches that remain relevant to current debates about how to manage security risks associated with emerging technologies in an era of renewed great power competition.

1) In the *unilateral access denial* approach, a country tries to keep sensitive technology away from everyone else solely through its own efforts. the United States had a monopoly on nuclear weapons in the late 1940s, it considered international control of atomic energy, but ultimately passed legislation and pursued other policies intended to keep weapons-related knowledge and technology away from all other countries. That effort failed rapidly, but the United States has still relied more heavily than most other countries on unilateral access denial as a major component of its efforts to control the spread of dangerous dual-use technologies. In some cases, this has included military attacks or sabotage of facilities where dual-use technologies might be used to develop weapons, as with the Stuxnet cyberattacks on centrifuges used by Iran to enrich uranium.

2) In the *allies versus adversaries* approach, like-minded countries with different levels of technological development collaborate and trade to build up their own group's military, economic, and scientific power while refusing to do so with potential adversaries. After World War II, the United States simultaneously tried to rebuild Western Europe economically and militarily, and to convince recipients of U.S. assistance to withhold sensitive technologies from

Soviet bloc states.[5] This approach can be difficult to sustain as more of the allies become capable of making the weapons and dual-use technologies themselves if they have different views on benefits and costs of denial for their security, economic, and political objectives.

3) The *suppliers against seekers* approach unites countries and companies with advanced capabilities, including non-allies, to prevent the spread of sensitive dual-use technologies to potential proliferators, even their own allies. The 1974 Nuclear Suppliers Group (NSG) brought so-called "first" and "second" world countries together to restrict exports of materials, components, and technologies that other countries might use to make nuclear weapons. This approach can be effective in the short term to the extent that there is unity among suppliers but discriminating between "haves" and "have nots" breeds resentment and motivates indigenous technology development efforts.

4) *Cooperative management* of dual-use technologies involves agreement on rules, typically about legitimate and responsible use rather than access, and on transparency arrangements among diverse groups of state and nonstate actors with varying security relationships, economic development levels, and indigenous technical capabilities. Such cooperative security arrangements found their fullest form in the early post-Cold War period, but versions of this more inclusive and consensual approach were proposed, and sometimes adopted, even when the world was divided into hostile blocs, most notably with the 1968 Nuclear Nonproliferation Treaty. Reaching consensus on the rules among a large and diverse group of actors is hard, having confidence that everybody is following the rules is harder, and responding effectively to non-compliance is especially difficult.

The next four sections explore why the United States chose one or a combination of these approaches for balancing the benefits and risks of different types of dual-use technologies at various times in the past. They compare and contrast how efforts to control the spread of nuclear technologies compared with those to control advanced conventional weapons and dual-use capabilities during the Cold War, and how the differing worldviews and national security strategies of the Clinton and George W. Bush administrations led to very different ways of trying to control technologies related to WMD.

These four historical cases show that which approach was chosen, and how well it worked to balance security, economic, and innovation objectives depended on four factors:

1) the current global security and economic context,
2) the characteristics of the technology in question,
3) the current state of technological development and distribution; and
4) the relevant stakeholders' interests and ideas about managing dual-use technology.

Although there are important differences over time in each of these four factors that shape the desirability and feasibility of different governance approaches, the dominant features that

[5] John H. Henshaw, "The Origins of CoCom: Lessons for Contemporary Proliferation Control Regimes," (Washington DC: The Henry L. Stimson Center, May 1993), 8-9. https://www.stimson.org/wp-content/files/file-attachments/Report7_1.pdf

characterize current emerging technology governance challenges were not completely absent from earlier iterations of this policy problem. For example, most of the historical efforts focused on controlling physical items to preserve U.S. advantage vis-a-vis a peer competitor or proliferators who might use WMD for an asymmetrical attack, whereas many currently emerging technologies of concern are digital, or intangible in other ways. From the earliest days of the nuclear age, though, there have been debates about whether to share sensitive knowledge about dual-use technologies in hopes of fostering cooperative governance arrangements, or to try to maintain secrecy and access control for as long as possible. There have also been debates about the benefits and risks of sharing technical knowledge and engaging in joint production with countries that were military allies and economic competitors. Governments were historically the driving force behind the development and diffusion of strategic technologies with major military applications, but commercial stakeholders also had varying levels of influence in different countries and under different economic conditions. Much like today, there were numerous previous instances where the United States wanted tighter controls on a larger set of dual-use and military exports than its allies or other suppliers did.

In short, many of the challenges associated with governance of "emerging" technologies today were foreshadowed decades ago, and many of the governance mechanisms developed then remain potentially relevant. It was rarely easy, though, to reach and sustain multi-stakeholder agreement on a particular set of governance arrangements. Furthermore, those arrangements were never fully able to control who had access to powerful dual-use technologies, or how they used them, yet they always imposed significant military, economic, technological or political burdens on those who implemented them. This experience should temper expectations about efforts to control emerging technologies today.

Nuclear technology governance during the Cold War

Nuclear physics posed a quintessential early challenge for governance of emerging technology. As soon as the Manhattan project demonstrated that nuclear technology could be used not only for peaceful purposes, but also to make weapons with unprecedented destructive power, a small group of American scientists, strategists, and policymakers began debating how to maximize the benefits and minimize the risks. Due to the rapidly deteriorating security environment after World War II and the U.S. government's monopoly on fissile materials and know-how needed to make nuclear weapons, those who argued for a *unilateral access denial* strategy initially prevailed over those who advocated for cooperative management. Developments outside of U.S. control, however, eroded the feasibility and desirability of that governance strategy. Within a few years of the first Soviet nuclear weapons test in 1949, the United States began moving toward the complex mix of governance mechanisms that are still being used today to reduce nuclear proliferation risks while encouraging peaceful commerce and scientific advancement.

The small group of U.S. government officials and scientists who knew about the development of nuclear weapons before the end of World War II argued about what to tell Stalin. Those who wanted to share information with the Soviet allies, such as Secretary of War Henry Stimson and scientist Robert Oppenheimer, argued that scientists around the world already understood

fundamental principles of nuclear physics, so the knowledge and materials needed to make nuclear weapons could not be kept from other countries for long. Before the first nuclear weapon test, they argued that the best chance of avoiding a nuclear arms race lay in sharing enough information to convince the Soviets that they should cooperate with the United States to establish an "Atomic Development Authority" with direct managerial control over all dangerous nuclear activities, rather than indirect oversight of national programs.[6] After atomic bombs were used against Hiroshima and Nagasaki, they convinced the advisory committee studying what type of controls on nuclear technology the United States should propose that direct international management of dangerous dual-use activities, like uranium enrichment and plutonium reprocessing, was the most realistic way to allow peaceful uses and prevent military applications.

Doubts about the viability of US-Soviet cooperation after they defeated their common enemies, and desires to prolong the U.S. nuclear monopoly for as long as possible, led the Truman administration to opt for a *unilateral access denial* approach instead. The 1946 Atomic Energy Act, which established civilian control over the U.S. nuclear program, also included a section specifying that all information about making nuclear weapons was automatically classified regardless of its source, unless specifically declassified by the Atomic Energy Commission. This tight control on "restricted data" precluded sharing information even with Britain and Canada, who had contributed to the Manhattan Project under a little-known agreement for post-war nuclear cooperation.[7] U.S. leaders opted for a nuclear governance strategy that seriously damaged relations with close allies because they falsely believed that the United States could corner the global market on uranium and that Soviet scientists and engineers were too backward to make nuclear weapons anytime soon.[8] They also failed to understand British leaders' high motivation to complete an indigenous nuclear weapons development effort if the Americans would not share sensitive nuclear information with them.[9] The assumptions underlying this unilateral control strategy were exploded a few years later by the first Soviet nuclear test in 1949 and British one in 1952.

President Eisenhower's 1953 Atoms for Peace speech was a very public acknowledgement that the *unilateral access denial* strategy had failed to preserve the U.S. atomic monopoly and that a more cooperative approach to the management of nuclear technology was needed. His call for the superpowers to donate some fissile material from their military stockpiles to an international agency that would distribute it for peaceful use was part of a public relations campaign to build domestic and international support for the rapidly expanding American nuclear deterrent, with little expectation that the Soviets would agree. Their stockpile of fissile material was much smaller than the U.S. stockpile was at this time, so the proposed equal contributions to an international fuel bank would impose greater constraints on their ability to manufacture weapons.

Eisenhower's speech prompted Congress and the National Security Council to consider how bilateral cooperation in civilian uses of nuclear technology could have economic, foreign policy,

[6] McGeorge Bundy, *Danger and Survival* (New York: Random House, 1988), 159.
[7] James Acton, "On the Regulation of Dual-Use Nuclear Technology," in Governance of Dual-Use Technologies: Theory and Practice, ed. Elisa D. Harris, (Cambridge: American Academy of Arts and Sciences, 2016), 16.
[8] Vince Houghton, *The Nuclear Spies* (Ithaca, NY: Cornell University Press, 2019), 167-169.
[9] Bundy, *Danger and Survival*, 461-70.

and security benefits. Congress amended the Atomic Energy Act in 1954 so that U.S. officials could share some nuclear information with foreign nationals and private companies interested in building and operating commercial nuclear reactors, on the condition that recipient countries accepted certain end-use requirements and safeguards.

A March 1955 National Security Council Directive spelled out the broader policy logic of conditional cooperation as an alternative to access-denial options. If managed carefully, civilian nuclear cooperation could advance nonproliferation objectives in addition to economic gains and foreign policy benefits (e.g. improving U.S. relations with recipient countries and countering Soviet efforts to gain influence by sharing their nuclear technology.) By helping foreign countries construct nuclear power and research reactors, the United States would gain insights into their nuclear activities, leverage over their policies, and opportunities to shape their management of dual-use capabilities to prevent diversion for military programs or re-export to countries of greater proliferation concern.[10]

Eisenhower also championed the establishment of the International Atomic Energy Agency (IAEA) in 1957. This multilateral mechanism for facilitating peaceful nuclear cooperation was negotiated under U.N. auspices among twelve countries who already had advanced nuclear programs (the United States, Britain, Canada, France and the Soviet Union), supplied uranium and thorium for nuclear reactors (Belgium, Australia, Portugal and South Africa) or sought nuclear assistance (India, Brazil, and Czechoslovakia).

The IAEA was inclusive, but weak compared with national nuclear suppliers. It was designed to be a "broker not a banker."[11] It helped arrange bilateral and multilateral deals, provided technical assistance, and applied safeguards when requested by the contracting parties. It did not have its own stockpile of fissile material to dispense, authority to impose a standard set of safeguards on all nuclear transactions, or any enforcement powers.[12] States remained free to conduct nuclear trade without requiring safeguards if they wished, and to pursue indigenous nuclear development for military purposes with unsafeguarded material and facilities sometimes co-located with safeguarded ones.[13]

The 1968 Treaty on the Nonproliferation of Nuclear Weapons (NPT) was a much more ambitious and effective cooperative control arrangement based on more equitable, consensually agreed rules about responsible management of dual-use technology. It created a set of interlocking legal obligations between states that had tested nuclear weapons before the NPT was agreed upon and those that had not. The nuclear weapons state (NWS) parties committed not to help non-nuclear weapons state (NNWS) parties acquire nuclear weapons and to assist them with

[10] Jonas Siegel, *U.S. Nuclear Energy Cooperation and Partner Country Nonproliferation: Cases from East Asia* Ph.D. dissertation, University of Maryland, 2022, 58-59.
[11] Paul C. Szasz, *The Law and Practice of the International Atomic Energy Agency,* Legal Series #7 (Vienna: International Atomic Energy Agency, 1970), 29.
[12] Bertrand Goldschmidt, "The Origins of the International Atomic Energy Agency," *IAEA Bulletin* 19:4 (August 1977).
[13] Lawrence Scheinman, "Cooperative Oversight of Dangerous Technologies: Lessons from the IAEA Safeguards System," *CISSM Working Paper* (January 2005), https://www.cissm.umd.edu/research-impact/publications/cooperative-oversight-dangerous-technologies-lessons-international.

peaceful nuclear programs on a non-discriminatory basis. They also promised to reverse the nuclear arms race and eventually eliminate their own arsenal as part of a general and complete disarmament accord. In return, the NNWS committed not to acquire nuclear weapons and to accept a standard set of IAEA safeguards on their entire nuclear program to confirm its purely peaceful nature. France and China could have joined as NWS but objected to the two-tiered structure of the NPT and refused to accede until the 1990s. A number of countries that had not yet tested nuclear weapons also did not join initially so as to keep their options open. Over time, though, the NPT has gained near universal membership (only India, Pakistan, Israel, North Korea, and South Sudan are currently outside of it), and high, if imperfect, levels of compliance.[14]

The NPT fits the *cooperative management* approach because it was open to all countries, regardless of nuclear status or stance in the Cold War confrontation, and because members voluntarily accepted an equitable set of interlocking rights and obligations. It is primarily a demand-side strategy because it seeks to reduce NNWS' desire to acquire nuclear weapons by reducing security-related motivations and strengthening normative disincentives. There is an obvious tension, though, between the NPT obligation for member states that could supply nuclear technology for peaceful purposes to assist NNWS on a non-discriminatory basis, and their obligation not to help additional countries acquire nuclear weapons. Thus, these countries supplemented the NPT with a *suppliers against seekers* arrangement known as the Zangger Committee. The committee initially agreed on a "trigger list" of dual-use nuclear materials and technologies that they would only supply if the recipient agreed to IAEA safeguards to ensure their purely peaceful use, regardless of whether that country had joined the NPT or not.[15]

India's purportedly "peaceful" nuclear test in 1974 underscored that nuclear materials and technologies acquired for civilian purposes could also advance weapon development. Canada, West Germany, France, Japan, the Union of Soviet Socialist Republics (USSR), the United States and the United Kingdom formed NSG in 1974. Its controls covered not only nuclear dual-use items but also non-nuclear dual-use items that could be used to make nuclear weapons. The NSG also required all recipient states to take nuclear security and physical protection measures and to make end use commitments.[16] From the suppliers' perspective, the NSG guidelines were useful for harmonizing export control practices even though the group did not meet after 1978.[17] The arrangement bred resentment among NNWS who could not purchase dual-use items because some NSG members questioned their true intentions even though they were deemed in compliance with IAEA safeguard obligations.

This short recap of control arrangements for dual-use nuclear technologies during the Cold War shows the pitfalls of unilateral action. The United States had a complete monopoly on critical

[14] James Walsh, "Learning from Past Success: the NPT and the Future of Non-Proliferation," (October 2005), WMDC paper no. 41 at: https://www.belfercenter.org/sites/default/files/legacy/files/wmdcno41.pdf
[15] "ZANGGER COMMITTEE (ZAC)," *NTI*, July 14, 2020, https://www.nti.org/learn/treaties-and-regimes/zangger-committee-zac/
[16] "NUCLEAR SUPPLIERS GROUP (NSG)," *NTI*, July 14, 2020, https://www.nti.org/learn/treaties-and-regimes/nuclear-suppliers-group-nsg/
[17] Acton, "On the Regulation of Dual-Use Nuclear Technology," p. 28.

aspects of weapons development, saw tremendous security value in preserving that advantage, and was willing to pay a high political price for refusing to share sensitive information, yet a purely *unilateral access denial* strategy backfired by motivating other countries to acquire their own nuclear weapons for security, economic, or political reasons.

The cooperative management approach initiated with the Atoms for Peace speech and institutionalized through the Nuclear Nonproliferation Treaty has had a much more profound and lasting effect on both countries' choices about how they will use nuclear technologies. It has also bolstered international confidence in the purely peaceful nature of most nuclear programs. This governance arrangement has important ambiguities and weaknesses that arise from compromises necessary to gain near-universal assent among a very diverse group of member states, and has been supplemented with various *suppliers against seekers* arrangements. Whether the added security benefits of coordinated denial by suppliers outweigh the economic and political costs, though, was unclear during the Cold War. As we will see below, contradictions between cooperative commitments to facilitate NPT-NNWS members' access to and assistance with nuclear technology for peaceful purposes and coordination among suppliers to deny certain types of nuclear sales to countries suspected of harboring secret nuclear weapons ambitions even though they were in compliance with the IAEA safeguards obligations has always caused friction, and became even more controversial after nuclear proliferation became a top security priority in the 1990s.

Cold War controls on non-nuclear dual-use technologies

U.S. officials' efforts to manage the spread of advanced non-nuclear dual-use technologies after World War II also occurred in a context of growing bipolar rivalry, though decision makers abandoned a purely unilateral approach in this sector quickly, too. The United States had a near-monopoly on advanced conventional military technology in the aftermath of World War II, but rather than trying to preserve that strategic advantage for as long as possible through *unilateral access denial*, it took the *allies versus adversaries* approach to export controls, opting to share capabilities and know-how with European and Asian countries to help them rebuild and rearm against communist countries. Successive U.S. governments had much more difficulty getting domestic and international agreement on a stable set of arrangements for managing trade in dual-use goods, services, and knowledge with conventional military applications than they did in the nuclear case. This is partly because the number of engaged stakeholders with different interests and ideas was larger, and partly because the United States relied more on coercive rather than cooperative control mechanisms, even as allied countries advanced technologically to the point where some of the dual-use capabilities that they wanted to sell around the world were as good or better than American products that the U.S. government still wanted to tightly control.

Initial U.S. efforts to structure the post-World War II order to promote peace and prosperity involved tension between an ideological commitment to free trade and a strategic perception, accurate or not, that the United States had gained wartime advantages through aggressive use of export controls to get concessions from other countries. The Truman administration initially extended wartime export controls to maintain an adequate supply of scarce items needed in the

United States for various purposes. By 1947, the rationale for continued reliance on export controls moved from scarcity after the last war to strategic advantage in the next one: U.S. leaders had decided that the Soviet threat warranted efforts to inflict "the greatest economic injury to the USSR and its satellites."[18] Congress passed the 1949 Export Control Act, granting peacetime authority to use export controls for national security, foreign policy, or economic reasons. Executive branch officials formulated lists (without industry input) of items that could improve communist countries' military capabilities. Export of items on the list was e prohibited or required a time-consuming and secretive case-by-case review process to get a license for export even to friendly countries.[19] But this comprehensive *unilateral access denial* approach conflicted with the Cold War objectives of creating a strong alliance system and rebuilding allies' economic and military capabilities, so the United States shifted to an *allies versus adversaries* approach.

The United States spearheaded the establishment of the Coordinating Committee for Multilateral Export Controls (COCOM) in 1949 to coordinate with its allies on controls of munitions, atomic energy, and industrial/commercial dual-use technology. Before approaching other European nations, the United States reached consensus with Britain and France on the general approach: the United States would sell advanced conventional weapons and share dual-use technologies with other COCOM members who agreed not to sell items that could improve potential adversaries' military capabilities.

All North Atlantic Treaty Organization (NATO) members (excluding Iceland), as well as Japan and Australia joined the informal arrangement within a few years. Most member governments besides the United States consulted closely with business leaders on export control policies, so COCOM was structured to minimize interference with trade. Each member maintained veto power over additions to the control lists, and was responsible for enforcement in its own jurisdiction. As the sole source of many items of military significance, though, the United States reserved the right to restrict exports of items not on the COCOM lists, even to its allies.[20]

At first, the U.S. government had considerable leverage over its European counterparts to coerce them into following more restrictive export practices towards the USSR, Warsaw Treaty Organization members, and the People's Republic of China (PRC) than they had agreed to through the COCOM list-making process. The Mutual Defense Assistance Control Act (or Battle Act) of 1951 authorized U.S. officials to withhold Marshall Plan assistance if a recipient country failed to adhere to export controls, linking aid to trade. The United States had a solid economic position with a strong market and the enviable status as the world's technological leader. In contrast, its Western European allies were still rebuilding their economies.[21] But, the most

[18] Report by the National Security Council, "Control of Exports to the U.S.S.R. and Eastern Europe," cited in William Long, U.S. Export Control Policy: Executive Autonomy the U.S.S.R. and Eastern Europe," cited in William Long, U.S. Export Control Policy: Executive Autonomy vs. Congressional Reform (New York: Columbia University Press, 1990), 15.
[19] Michael Mastanduno "The United States Defiant: Export Controls in the Postwar Era," *Daedalus*, Vol. 120, No. 4, Fall, 1991, 92.
[20] Mastanduno, "The United States Defiant," 97.
[21] Kevin F. F. Quigley and William J. Long, "Export Controls: Moving Beyond Economic Containment" *World Policy Journal*, Winter, 1989/1990, Vol. 7, No. 1, 169.

important factor enabling the United States to organize a broad multilateral embargo strategy in the early years of COCOM was shared threat perceptions. During the Korean War, COCOM members suspected that the Soviets were preparing for a general war, and thus agreed that communist countries were worthy targets for economic warfare.[22] That consensus started to soften after the Korean armistice in 1953.

As fear of general war waned and the defense focus turned toward nuclear deterrence, the costs of the broad embargo strategy became unpalatable to many Western European allies. U.S. industry did not have a substantive stake in Eastern European markets in the 1950s, and the USSR and PRC were deliberately trying to isolate their economies from the capitalist system. By this time, though, many Western European countries had established significant trade relations with Soviet satellite countries on key imports such as coal and timber. Economic recovery in Europe and U.S. sharing of defense technology with allies were increasing suppliers of militarily significant goods and eroding the U.S. technological dominance.[23] West European officials also saw much greater risk than their American counterparts in provoking the Soviets through economic warfare because of their close proximity.[24] As Eastern European demand for technology grew, COCOM reduced the number of items controlled in 1954, 1957, and 1958.[25]

The United States did not make corresponding cuts to its own export list in the 1950s, with damaging economic effects for U.S. suppliers' ability to sell abroad. Right after World War II, the value of exported goods as a share of gross domestic product (GDP) had been 4.2% for the United States, equivalent to both the global average and the percentage for Germany. By 1960, the value of German exports had risen to 15.8% of GDP, and the global average had climbed to 8.7%, while the value of U.S. exports had declined to 3.8% of its GDP.[26] U.S. suppliers lost market share because the U.S. government continued to take longer than COCOM partners did to review and approve exports to low-risk destinations. It routinely asserted authority to control the reexport of U.S.-origin technologies, components, and products even if they were not on the revised COCOM lists. It tried to pressure countries like Sweden and Switzerland who were not COCOM members to apply COCOM trade controls. It sometimes even applied U.S. export controls directly against COCOM members whose implementation of restrictions it viewed as too lax.[27]

By the 1960s, the United Kingdom, France and West Germany were also developing military aircraft and tanks as alternatives to options available from U.S. suppliers, often sharing costs and benefits through co-production agreements. Many COCOM members were also manufacturing dual-use products that the United States still thought should be controlled. As U.S. technological superiority eroded, growing divergence between multilateral and unilateral export controls put

[22] Michael Mastanduno, "Trade as a Strategic Weapon: American and Alliance Export Control Policy in the Early Postwar Period," *International Organization*, Winter, 1988, Vol. 42, No. 1, 123.
[23] Reinicke, "Political Economy of Nonproliferation," 176, and "Arming our Allies," 21.
[24] Quigley and Long, "Moving Beyond," 169.
[25] Gunnar Adler-Karlsson, *Western Economic Warfare*, 1947-1967 (Stockholm: Almquist and Wiksell, 1968).
[26] Estaban Ortiz-Ospina and Diana Beltekian, "Trade and Globalization," chart 2, last updated 2018, at: https://ourworldindata.org/trade-and-globalization.
[27] Mastanduno, "The United States Defiant," 97-8.

U.S. firms at an increasing economic disadvantage. It also diminished whatever security benefits might have been achieved through a more unified approach.

Dissatisfaction with U.S. export control policies grew, but various U.S. stakeholders disagreed about how to prioritize competing objectives, making it harder to craft U.S. export control policies that garnered broad support at home and acquiescence from dependent allies. U.S. industry and the Commerce Department argued for trade liberalization on economic grounds. During détente, the White House and State Department wanted to condition relaxation of export controls on foreign policy concessions by the Soviet Union, while DOD consistently pursued highly restrictive practices for national security reasons.[28]

Congressional actions during the 1960s illustrate these competing concerns. Congress initially preferred the status quo: it passed legislation in 1962 preventing the Executive branch from making trade concessions to improve political relations with Eastern bloc countries. Stakeholder preferences regarding the relative importance of security, economic, and political considerations in U.S. export control decisions shifted somewhat during the 1960s, though, as the Vietnam war caused budget problems, tensions with the USSR eased, and global economic competition increased. Congress also became more responsive to industry concerns as the contribution made by trade to U.S. GDP growth fell further behind other industrialized countries.[29] By 1969, the German percentage was almost 20% while the U.S. trade contribution to GDP remained at 3.8%). That year, Congress passed the Export Administration Act (EAA), which directed the Executive branch to reduce the burden of export controls on U.S. industry. It retained export controls on all communist countries but specified that when determining whether to block the transfer of a specific item, the government must consider whether a comparable item was available from a foreign source in sufficient quantities to make U.S. restrictions ineffective. If so, the president could still restrict export of that item, but had to report the reason to Congress.[30]

Over the next decade, U.S. export control policies were relaxed somewhat for economic and foreign policy reasons as private industry spending on R&D pulled even with government spending, and business leaders gained more clout with Congress.[31] For example, while high-speed computers were tightly controlled for national security reasons, some COCOM countries were selling lower-end computers to Eastern bloc countries. U.S. firms wanted a share of that business, and successfully lobbied for U.S. government approval.[32] In the first half of 1970, U.S. businesses received COCOM exceptions for $18.6 million in computer exports, compared to only $1.5 million total in 1969.[33] The Nixon and Carter administrations used selective export authorizations to improve U.S. relations with some Eastern bloc countries and to gain foreign policy concessions from the USSR. In 1977, Congress ended the practice of treating all

[28] ibid. 105.
[29] Ortiz-Ospina and Beltekian, "Trade and Globalization."
[30] Sayles, "The U.S. Export Control System," p. 4.
[31] National Center for Science and Engineering Statistics, "National Patterns of R&D Resources, 2019-20 Data Update," NSF-22-320 (February 22, 2022) at: https://ncses.nsf.gov/pubs/nsf22320.
[32] Frank Cain, "Computers and the Cold War: United States Restrictions on the Export of Computers to the Soviet Union and Communist China," Journal of Contemporary History , Jan., 2005, Vol. 40, No. 1 (Jan., 2005), 142-3.
[33] ibid.

communist countries alike for export control purposes. It directed regulators to make case-by-case decisions based on the intended recipient's current and potential future relationships with the United States, its allies, and its adversaries, and on its willingness to follow U.S. policies regarding retransfers to other countries. The 1979 Export Control Act continued this liberalization trend.[34]

Détente also brought some short-lived, controversial gains in scientific collaboration involving dual-use technologies. Even at the height of the Cold War, the superpowers had engaged in some scientific cooperation with potential military implications, such as joint effort to develop vaccines for polio in the 1950s and smallpox in the 1960s.[35] Joint scientific research between the National Academy of Sciences (NAS) of the United States and the Academy of Sciences of the USSR began in 1959.[36] As relations improved, international scientists hoped that more ambitious forms of cooperation might become possible. In 1970, the British requested U.S. approval to sell high-speed computers containing U.S. components to the Institute of High Energy Physics in Serpukhov.[37] The Defense Department, the Joint Chiefs of Staff and the Atomic Energy Commission all strongly opposed the sale on national security grounds. The State and Treasury Departments and the Office of Science and Technology (OST) favored approval for strategic and economic reasons after determining that safeguards proposed by the British would adequately limit the risk that the computers would be applied to missile system design instead of civilian research. President Nixon eventually sided with State, Treasury and OST, and allowed the sale to be completed.[38]

The backlash against détente in the mid-1970s stoked fears that the Soviets were closing the technological gap through licit and illicit means, countering economic and foreign policy rationales for export control liberalization.[39] DOD highlighted the national security risks posed by the open exchanges between Soviet scientists and American industry and the potential for knowledge transfer on sensitive technologies.[40] In 1976, the Defense Science Board recommended placing export controls on intangibles like "design and manufacturing know-how" of dual-use technologies. A task force chaired by J. Fred Bucy, an executive at Texas Instruments, called for export reforms that reduced control on products available from foreign suppliers and added restrictions on cutting-edge technologies. It found that "for the most critical technologies, the United States should not release know-how beyond its borders, and then depend on COCOM for absolute control." Moreover, it maintained that the United States should

[34] Sayles, "The U.S. Export Control System," p. 4.
[35] P.J. Hotez (2014). "Vaccine diplomacy": historical perspectives and future directions. *PLoS neglected tropical diseases*, 8(6), e2808. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4072536/
[36] Glenn E. Schweitzer, "US-Soviet scientific cooperation: The interacademy program," *Technology in Society*, vol. 14, Issue 2, 173.
[37] Cain, "Computers and the Cold War", 144
[38] ibid., 146
[39] Thomas-Noone, "Cold War can teach."
[40] Michael Mastanduno, *Economic Containment*, (Ithaca: Cornell University Press, 1993), 186.

export to countries outside of COCOM "only the technology we would be willing to transfer directly to Communist countries."[41]

The Carter administration directed federal agencies to develop a list of critical technologies that should be withheld from adversaries, but decided that the economic and diplomatic costs of also denying access to allies would outweigh potential security benefits. Numerous agencies added whatever new technologies they thought might have military benefits, with little regard for whether effective control was actually feasible. What began as an effort to streamline and modernize U.S. export rules ended by adding extensive new technology controls to existing ones on military and dual-use products.[42]

The United States increased sanctions on the Soviet Union in response to its 1979 invasion of Afghanistan and started using export controls as leverage for many other foreign policy objectives besides anti-Communism. It sanctioned Uganda, South Africa, Chile, Iran, and Pakistan, among others, for violating human rights, supporting terrorism, pursuing nuclear weapons, and other objectionable behavior.

At the same time, the United States was starting to relax export restrictions on the People's Republic of China following its 1978 decision to open up to the rest of the world, and 1979 normalization of US-China relations, in the hope that economic engagement with the West would widen the Sino-Soviet split.[43] The Carter administration had used technology cooperation with China as an inducement to align more with the United States against the Soviet Union, and offered to sell China a communications satellite. Still, the Chinese sought technological and economic benefits from learning how to make their own satellites, and made a major investment in developing indigenous space capabilities after President Reagan rebuffed their request for technological assistance. A few years later, though, Reagan allowed China to launch an American commercial communications satellite in return for curtailing missile sales to Iran.[44] The United States also sold some military items to the People's Liberation Army during the Reagan years, a form of trade liberalization that ended in 1989, when Congress banned all military sales to China as a sanction for the Tiananmen Square massacre.

After decades of touting how heavy government spending on military R&D had "spin-off" benefits for commercial products, by the 1980s the U.S. military was beginning to reap "spin-on" benefits by purchasing off-the-shelf commercial items that offered greater capability at lower cost. Some Japanese high-tech companies offered superior products compared to their American counterparts, though, in key areas like semiconductors and micro-electronics. The Reagan

[41] Office of the Director of Defense Research and Engineering, *An Analysis of Export Control of U.S. Technology - A DOD Perspective: A Report by the Defense Science Board Task Force on Export of U.S. Technology,* by J. Fred Bucy, 1976. https://apps.dtic.mil/dtic/tr/fulltext/u2/a022029.pdf
[42] Mastanduno, "The United States Defiant," 101-3.
[43] Sally A. Meese, "Export Controls to China: An Emerging Trend for Dual-Use Exports," *Maryland Journal of International Law,"* 7:1 (1981)
[44] Gregory Kulacki, "Chinese Intentions in Space: A Historical Perspective for Future Cooperation," *Space and Defense* (Winter 2010), pp. 103-8.

administration wanted to help American high-tech firms gain market share and meet more U.S. military needs, without getting the government too involved in the private sector.[45]

During the Reagan administration's defense build-up, the United States substantially increased how much military equipment it bought from European companies, which could make many military products that rivaled American-made options by then. It also initiated co-development projects with NATO allies involving major financial investments and transfers of critical technical information. The trade imbalance between the United States and Western Europe for military equipment went from 7:1 in the late 1970s to 2:1 a decade later.[46]

While the Reagan administration was working to ramp up NATO military capabilities, it was also trying to punish European allies for circumventing U.S. policy on dual-use technology transfers to advance their own industries.[47] It established the BIS to separate the Commerce Department's export control enforcement responsibilities from the trade promotion activities carried out by the International Trade Administration. It used EAA amendments passed in the mid-1970s to move the export control process further back toward economic warfare and *unilateral access denial*. Top Defense Department officials, including Secretary Caspar Weinberger and Assistant Secretary Richard Perle, prioritized tightening export controls on both communist and noncommunist countries. They formalized DOD's role in the export review process, giving it a functional veto over proposed sales to Eastern bloc countries. They also caused a diplomatic uproar by retroactively applying newly asserted authority to regulate exports of U.S-owned subsidiaries in foreign countries, then sanctioning European companies that helped build a gas pipeline from Siberia.[48]

The Reagan administration also took steps to restrict foreign scientists and companies from gaining sensitive knowledge by interacting with American academics and hiring U.S. experts. It established the Technology Transfer Intelligence Committee to review visa applications for Soviet scientists interested in attending academic conferences in the United States in scientific areas relevant to national security (i.e., robotics, nuclear fusion, etc.)[49] It tried to restrict publication of research on dual-use technologies in ways that academic leaders considered ineffective and harmful to technological innovation.[50] It even forced a British firm to obtain export licenses for the knowledge gained hiring American engineers.[51]

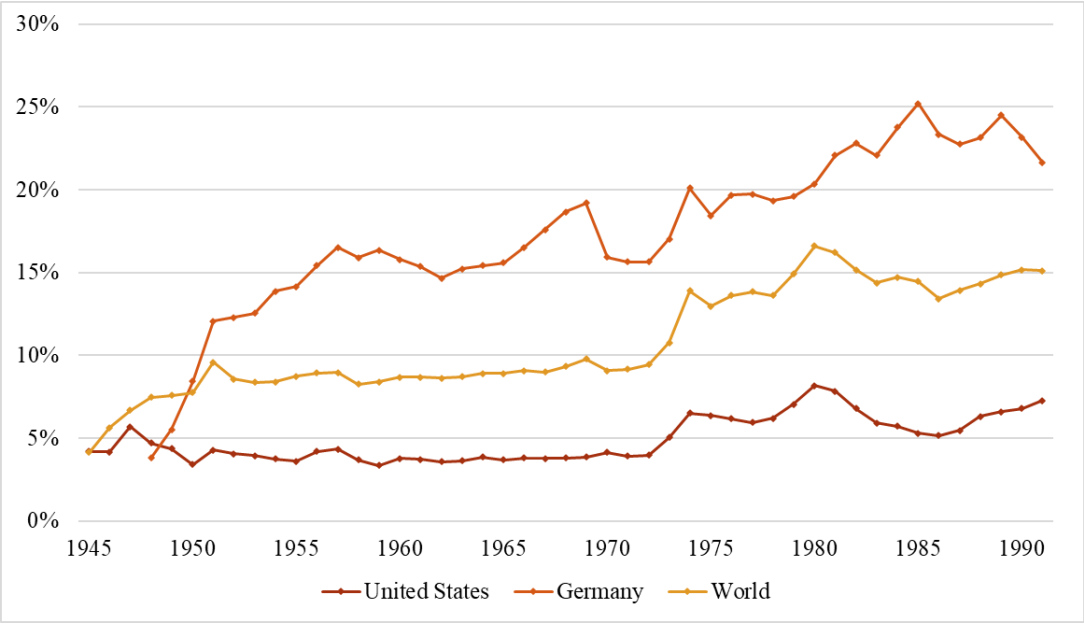
U.S. officials and security experts considered the advantages in several key dual-use technologies related to missile accuracy, including computer technology and microelectronic miniaturization, that the United States and some allies enjoyed over the Soviet Union to be particularly important at this time, but Donald MacKenzie found that Western debates about how

[45] Judith Reppy, "Managing Dual-Use technology in an Age of Uncertainty," *The Forum* 4:1 (2006), 2.
[46] Arming our Allies, p. 13.
[47] Mastanduno, "United States Defiant," 96.
[48] Paul Lewis, "A Soviet Project Tempts Europe," *The New York Times* (May 30, 1982), sec 3, p. 7.
[49] Thomas-Noone, "Cold War can teach."
[50] "Appendix G LETTER FROM FIVE UNIVERSITY PRESIDENTS," in Scientific Communication and National Security, *The National Academy Press*, 1982, 136.
[51] Mastanduno, "The United States Defiant," 105-6.

to protect this advantage were "based on a naive view of the nature of technology transfer."[52] Western analysts underestimated how much Soviet scientists and engineers had learned about missile guidance from German experts after World War II. They exaggerated the significance of some technological constraints, such as problems the Soviets encountered with precision metal machining of ball bearings. Western analysts often disregarded social and organizational reasons that explain why the Soviets might favor "hardware" rather than "software" solutions to guidance problems, prompting them to design stellar-inertial guidance systems for submarine-launched ballistic missiles in ways that did not require as much advanced computer power as U.S. designs did. They attributed too much significance to Soviet acquisition of missile guidance technologies acquired from the West by licit and illicit means, leading them to believe that tightening export controls could slow Soviet progress in this field more than it did. Finally, they assumed unrealistically that it was still possible to prevent the Soviets from acquiring state-of-the-art dual-use technologies, such a key component for the airborne inertial navigation system that had been widely used in Boeing 747 airplanes since the early 1970s.[53]

Any security benefits from these draconian measures came at a heavy economic cost for the United States, as shown by Figure 1. With other high-quality options available on the international market, foreign customers moved away from U.S. sources of supply in most export-controlled sectors. U.S. exports as a share of GDP dropped from 8.2% in 1980, about half the global average, to 5.2% in 1986, when the global average was 13.4%.[54]

Figure 1. Value of exported goods as share of GDP, 1945 to 1991
Estimates correspond to merchandise export-to-GDP ratios.



Source: Fouquin and Hugot (CEPII 2016)

[52] Donald MacKenzie, "The Soviet Union and Strategic Missile Guidance," *International Security* 13:2 (Fall 1988) p. 8.
[53] MacKenzie, "The Soviet Union and Strategic Missile Guidance," p. 48.
[54] Ortiz-Ospina and Beltekian.

The Reagan administration's tight export controls began to be scaled back in 1987, after the U.S. trade deficit hit record levels. That year, the superpowers signed the Intermediate-range Nuclear Forces treaty, signaling a shift from superpower competition toward arms control, and Weinberger resigned, reducing the power of unilateralists in inter-agency export control debates. The following year, Congress amended the EAA to specify that export controls could not be maintained for national security reasons if comparable products were available from other countries. This started the value of exported goods relative to U.S. GDP on an upward trajectory, hitting 6.8% in 1990 and continuing to rise after the Cold War ended.

As concerns about superpower competition started to fade, worries about regional powers acquiring ballistic missiles capable of carrying nuclear weapons rose. Also in 1987, the seven most industrialized countries in the U.S. alliance system formally established the Missile Technology Control Regime (MTCR). These countries had decided to form an entity similar to the Nuclear Suppliers Group to coordinate decisions about selling missiles and dual-use space technologies after India successfully tested a space launch vehicle, South Korea tested a ballistic missile, and several other regional powers sought to acquire rockets from European firms.[55] MTCR members initially pledged to rarely, if ever, approve sales of ballistic missiles capable of carrying a 500 kg payload over 300 kilometers to non-members, and to use caution when transferring relevant dual-use technologies and components. Over time, both the scope and the membership of the MTCR expanded. In 1993, members agreed not to transfer any type of ballistic missile or unmanned aircraft to countries thought to have WMD programs. More NATO countries and non-aligned European states joined in the early 1990s, followed by Argentina in 1993, Brazil and Russia in 1995, and several other former Warsaw Pact countries in the late 1990s. Thus, the formation of the MTCR initiated a process that paralleled a broader post-Cold War re-orientation of U.S. export control efforts from the primary objective of strategic advantage in superpower competition to the primary objective of reducing risks associated with WMD proliferation.[56]

This review of Cold War export control arrangements for dual-use technologies related to advanced conventional weapons illustrates both the strategic appeal of taking an *allies versus adversaries* denial approach, and the practical difficulties of getting stable agreement among stakeholders about how to balance security, economic, political, and technological objectives. Unlike the nuclear case, where the United States decided early on that a *cooperative management* approach was its best option for managing the spread of dual-use capabilities in a highly competitive security context, the conventional case shows more controversy and fluctuation over time. It was much harder to get agreement between various U.S. and allied stakeholders about what should, or should not, be sold or shared with Communist countries. Frequent U.S. reform efforts did little to dampen dissatisfaction with any type of denial-based export control arrangement's effectiveness at enhancing security without causing unwarranted

[55] Dinshaw Mistry, *Containing Missile Proliferation: Strategic Technology, Security Regimes, and International Cooperation in Arms Control* (Seattle: University of Washington Press, 2003), 45-48.
[56] Department of State Bureau of International Security and Nonproliferation, *Missile Technology Control Regime (MTCR) Frequently Asked Questions [Fact Sheet]* https://www.state.gov/remarks-and-releases-bureau-of-international-security-and-nonproliferation/missile-technology-control-regime-mtcr-frequently-asked-questions/

economic, political or technological damage. Instead, each attempt to liberalize export control rules, harmonize U.S. and allied judgments, and streamline bureaucratic processes generated political pushback from those who feared that rivals would take advantage of increased trade and scientific exchange to narrow technological gaps with the West and build more formidable military capabilities.

Post-Cold War controls on WMD-related technologies

This pattern repeated in the early 1990s, as economic globalization increased incentives for U.S. trade liberalization at the same time that the main security driver for controls on dual-use technologies shifted from great power competition to WMD proliferation. U.S. government officials and security experts largely agreed on the key features of the new global economic and security context, but differed in their preferred response. The contribution of trade to GDP growth had been steadily rising for most countries since the early 1970s, but not for the United States, raising concerns that the world's pre-eminent military power was losing economic and technological leadership to Japan and Germany. Large-scale nuclear or conventional war now seemed highly unlikely, so the main motivation for strategic trade controls shifted to keeping WMD, and the means to make and deliver them, away from so-called "rogue states" and terrorist groups that might use them asymmetrically. Initial consideration of small-scale reforms soon led to more fundamental rethinking of how to balance security, economic, political, and technological considerations in the post-Cold War context. The Clinton administration tried a more cooperative approach to management of dangerous dual-use technologies, in the hope that all major countries could work together to create a peaceful, liberal order based on free markets, trade, democracy, and the rule of law. In keeping with its more unilateralist national security strategy, the George W. Bush administration favored unilateral access denial, coercive counterproliferation, and voluntary coalitions of like-minded countries.

Reconceptualizing technology governance for a new security and economic context

Even before the Soviet Union collapsed, members of Congress began asking fundamental questions about whether cooperating with allies on the development and production of advanced military capabilities still served U.S. interests. The Congressional Office of Technology Assessments provided an ambivalent assessment in its 1990 report, *Arming our Allies: Cooperation and Competition in Defense Technology*. It argued that the policy of collaborating with European and Asian countries in defense technology to build up alliance capabilities achieved its primary objective during the Cold War, but had unintended consequences that were becoming more problematic. U.S. willingness to share defense technologies with allies had been premised on the United States remaining at least one generation ahead of its European and Asian partners, but "the loss of technological supremacy may be an unavoidable long-term cost of maintaining strong security alliances."[57] Losing that technological edge further reduced the U.S.

[57] OTA, *Arming our Allies*, 3-5.

government's ability to control sales of dual-use technologies when it disagreed with allied governments about whether security risks outweigh economic benefits.

The development of sophisticated centers of defense technology outside the United States meant that there was "significant peacetime overcapacity" in the defense sector, and "intense international competition for sales of high technology weapons." In some cases, DOD could get better weapons at lower cost through international collaboration, but this would erode the U.S. defense industrial base over time. Moreover, foreign companies' willingness to sell advanced military capabilities to a wide range of customers might complicate the United States' ability to "project power into regions and against companies that have been armed by the Europeans." In short, while continued close defense collaboration with foreign partners "makes business sense for individual companies, it may ultimately create unacceptable dependence on foreign suppliers, erode parts of the U.S. defense industrial base, and undermine U.S. foreign policy goals such as the nonproliferation of delivery vehicles for WMD."[58]

A 1991 NAS report on export controls recommended a "paradigm shift" from a "denial based regime" to an "approval based regime" in which the Soviet Union and other former adversaries targeted by export controls would become partners in supply-side coordination to prevent or slow WMD proliferation.[59] It argued that current U.S. efforts to deny a broad range of dual-use technologies to Eastern bloc countries were neither feasible nor desirable. Feasibility – e.g., the "controllability" of military items and dual-use technologies – was not only a function of foreign availability. It also included the number of suppliers and seekers for a particular capability (in general, fewer stakeholders enhanced controllability), the extent to which other suppliers would implement export controls, whether unique items were traceable or easily concealed, whether objects of concern had become mass-produced commodities, whether they involved hardware or software, and more. The report defined desirability as the net effect on national interests when potential security benefits were weighed against negative effects of U.S. export controls on foreign relations with other suppliers and target countries, and negative economic impacts, including market share for U.S. firms, trade balances, and health of the U.S. defense industrial base.

The report's recommendations were more evolutionary than revolutionary, though. It maintained that narrowly tailored export controls could have a net positive effect on national security by slowing, if not permanently stopping, significant improvements to potential adversaries' military capabilities. It called for a larger voice for industry in export control policy, a stream-lined regulatory process in the United States, and agreement among COCOM members on a much smaller list of military items that should not go to particularly problematic actors. West-East trade should be encouraged unless it would directly provide the Soviet military or an aggressive player with significantly improved weapons. The report recommended that supply-side controls to constrain WMD proliferation be focused only on denying access to narrowly prescribed military activities and items required directly for weapons systems, with demand-side incentives addressed through the NPT and other cooperative nonproliferation agreements. It also advised that export controls imposed to sanction undesirable behavior be multilateral whenever

[58] ibid.
[59] NAS, "Finding Common Ground."

possible, and focused on punishing violations of international agreements and widely accepted norms.

George H. W. Bush's administration did decide to support replacing the extensive existing COCOM list of dual-use technologies that were supposed to be regulated with a much more selective "core list" of sensitive technologies that should still be carefully controlled. It did not, however, follow the recommendations to keep export controls imposed for nonproliferation purposes tightly focused on a list of militarily necessary items that were being sold by other suppliers. Shortly thereafter, though, Iraq's defeat in the 1991 Persian Gulf War revealed its clandestine nuclear, chemical, and biological weapons development efforts. The Bush administration's Enhanced Proliferation Control Initiative quickly imposed new unilateral trade controls on a wide range of high-tech dual-use exports, including chemical processing and fermentation equipment. It also expanded the list of restricted recipients from about ten countries widely suspected of proliferation (Argentina, Brazil, India, Iran, Iraq, Israel, Libya, Pakistan, South Africa, Syria) to more than twenty countries.

U.S. high-tech companies supported the nonproliferation objectives of export control reform, but criticized the administration's *unilateral access-denial* approach, suggesting that this would "penalize the good guys" who had not sold dangerous dual-use equipment to Iraq for the "sins of the wicked" European companies that had.[60] This set the stage for a fundamental rethinking of how the changed security and economic environment affected both the types of dual-use technologies that needed to be controlled and the means that should be used to manage them, along the lines of the "paradigm shift" recommended by the NAS report.

By the time William J. Clinton took office, some contributors to the 1991 NAS report had concluded that powerful trends associated with globalization made all three forms of technology denial strategies -- *unilateral access denial, allies versus adversaries,* and *suppliers against seekers* – not only unworkable, but also counter-productive. John Steinbruner, Ashton Carter, and William Perry, three security experts with policy experience, were leading a consortium of scholars and practitioners who were arguing that some type of global cooperative security system should replace the bipolar military confrontation of the Cold War. This group argued for expanding the multilateral cooperative management strategies developed for nuclear technology to cover other types of advanced dual-use technologies, including chemical, biological, and digital capabilities. The Clinton administration made some progress working with former adversaries, rising powers, and private corporations on new ways to accelerate global economic growth and technological innovation without increasing shared security risks. But technological capabilities advanced and spread much faster than global governance mechanisms improved.

The cooperative security consortium maintained that the changed geopolitical and economic context and the characteristics of WMD-relevant technologies required much more fundamental changes to export control systems than the 1991 NAS report had recommended. This group of independent academic experts agreed on the premise that secrecy and access denial could not be sustained for long in a tightly interconnected, information-driven global economy. They also

[60] Eliot Marshall, "War with Iraq Spurs New Export Controls," *Science* (February 1, 1991).

believed that most, if not all, of the former "second" and "third" world countries would move quickly to join COCOM countries as fully democratic members of a global free market and a rules-based international order working together on global challenges like civil violence and climate change. These countries would collectively have the vast majority of the world's military, economic, and scientific power. Therefore, their biggest security problem was managing the spread of powerful dual-use technologies so "rogue states" willing to violate the rules of the "new world order" could not acquire WMD that could offset the combined conventional capabilities of the law-abiding countries.[61]

Regardless of how closely governments coordinated on supply-side controls, this group argued that efforts to deny countries like Iraq, North Korea, and Iran WMD-related dual-use technology would be prohibitively expensive and ineffective. People and information could now move easily around the world. Global economic integration went beyond increasing flows of goods across borders, facilitated by a world-wide financial system with the U.S. dollar as the dominant reserve currency and the common denominator used for trade and other financial transactions. Internationalization of production due to foreign direct investment had become a major feature, too, further limiting national governments' ability to control who had access to high-tech knowledge and products.

As governments reduced defense spending, they also lost influence over technology development and commercialization. An increasingly independent private sector was driving major developments of dual-use technologies, with more attention to global commercial markets than to national military contracts.[62] The share of R&D spending by industry as a percentage of GDP increased significantly during the 1990s, while government spending declined steadily; by 1996, private sector R&D expenditures were twice the federal government's.[63] New internet companies such as Google were far less (if at all) reliant on government funding for their commercial activities, which reduced U.S. government leverage. Moreover, multinational corporations and other private sector actors could now trade and invest almost anywhere in the world, making it increasingly difficult for national governments to track and regulate their activities. In the Information Age, more of what governments might want to control was digital rather than physical, which facilitated the global diffusion of technology. And, more high-tech components had legitimate uses in both civilian and military sectors.

Under these circumstances, members of the cooperative security consortium argued that efforts to deny some countries access to potentially beneficial nuclear, chemical, and biological technologies would be counterproductive. Discriminatory rules regarding access to dual-use technologies would breed resentment and spur indigenous technology development, often undertaken secretly so that outsiders would have no ability to influence how increasingly sophisticated capabilities might be used. They advocated for a much more collaborative approach: working with all stakeholders, be they former adversaries, developing countries,

---

[61] Janne Nolan, ed., *Global Engagement* (Washington, DC: Brookings, 1994).
[62] Dan Steinbock, "The Challenges for America's Defense Innovation," ITIF Report, November 2014, https://itif.org/publications/2014/11/21/challenges-america%E2%80%99s-defense-innovation/.
[63] "Federal Policies and Innovations," *Congressional Budget Office*, November 2014, 11, https://www.cbo.gov/sites/default/files/113th-congress-2013-2014/reports/49487-Innovation.pdf

private companies, or academic experts, to maximize shared benefits from rapid technological advances in many fields, while engaging in an inclusive diplomatic process to define what constituted "responsible" behavior with dual-use technologies, and what was unacceptably threatening or risky.

Wolfgang Reinicke, the member of the cooperative security consortium who offered the most detailed alternative to denial-based export control arrangements, proposed supply- and demand-side strategies to facilitate most international trade, investment, and scientific collaboration involving WMD-relevant technologies, while using systematic disclosure requirements to prevent and protect against misuse. In a global economic, financial, and information environment, Reinicke argued, preventive regulation should focus on reducing the information asymmetries that proliferators used to acquire components for WMD disguised as legitimate transactions, making it easier for authorities to detect and disrupt suspicious patterns of activity.

Reinicke's proposal involved harnessing the growing power of information technology to synthesize insights from different types of state and nonstate actors involved in sales of dual-use technologies. Much of the information that authorities needed to know about the parties to and nature of such transactions could be collected directly from firms if sellers were required to enter information into a confidential database that officials could cross-check with other data to identify suspicious patterns. The World Bank and other lenders typically require detailed information from prospective borrowers, and could be required to evaluate proliferation risks as part of routine due diligence. Information gleaned from existing anti-money laundering requirements could be used to alert banks if a potential customer was a suspected proliferator, and to warn regulators before dual-use items had been delivered to somebody who might misuse them. If officials also shared more sensitive information with companies and financial institutions, about front companies, shady dealers, and illicit programs in countries of concern, legitimate actors could make more informed business decisions to avoid unwittingly aiding proliferation. Some companies and banks who might be tempted not to ask questions would be deterred because failure to satisfy disclosure requirements would open them to scrutiny from regulators. Those who went ahead with illicit transactions would also run the risk of more law-abiding business competitors informing officials who could impose hefty penalties. In short, by building a world-wide web of information about actors and activities involving dual-use technologies, regulators could minimize proliferation, a serious negative externality of global markets, while letting most people, money, knowledge, and products move freely throughout the system.[64]

The logic for *cooperative management* harkened back to the Acheson-Lilienthal Committees recommendations of international managerial control of atomic energy and the Eisenhower administration's rationale for using nuclear cooperation to shape nonproliferation policies and practices. Proponents maintained that state and nonstate actors involved in cooperative management of nuclear, biological, space, and other powerful dual-use technologies would internalize norms of responsible behavior, share sensitive information to reassure each other that they were following those rules, and build confidence by cooperating on increasingly ambitious

[64] Reinicke, "Cooperative Security and the Political Economy of Nonproliferation."

joint projects. They would prevent security threats from emerging by sharing sensitive information to make it harder for proliferators to hide illicit activities, and by conditioning international assistance on responsible behavior with WMD-related technologies. They would also protect each other by threatening collective action (fines, sanctions, or military operations) against anyone who violated the rules. If such a cooperative management regime could be established, advocates maintained, it could increase security, economic prosperity, and technological innovation simultaneously, instead of forcing contentious tradeoffs among these objectives.

Clinton's combination of cooperative management and suppliers against seekers

The Clinton administration generally embraced the view that promoting free trade and technological cooperation could enhance security as well as prosperity under post-Cold War conditions. Not only had tight export controls contributed to record U.S. deficits during the Reagan administration, but Japan's share of the global market for high-tech goods had also surpassed the United States' share.[65] Several assessments argued that excessive domestic export controls were needlessly stifling U.S. economic growth, particularly in high-technology industries. For example, a report by the Institute for International Economics blamed three-fourths of a $25-40 billion shortfall in 1993 on export controls.[66] The Clinton administration tried to use more *cooperative management* techniques to liberalize trade in dual-use technologies, but parts of DOD and State that cared more about preventing WMD proliferation than promoting trade pressed for more *suppliers against seekers* coordination, generating tensions between cooperative and coercive strategies for managing dual-use technologies. Its efforts to leverage technology cooperation both to improve overall security relations with Russia and China, and to incentivize them to be more selective regarding exports to potential proliferators were further complicated by pushback from members of Congress concerned about preserving U.S. technological and military advantages to head off future challenges from a resurgent Russia or a rising China.

To reconcile its security, economic, and foreign policy objectives, the White House tried to streamline export controls for lower-risk items while tasking the new interagency Trade Promotion Coordinating Committee with creating a unified framework for increasing U.S. exports abroad, including high-speed computers.[67] Clinton officials transferred some dual-use technologies, including communications satellites in 1996, from the more restrictive U.S. Munitions List (USML) administered by the State Department to the Commerce Control List (CCL), with an interagency process to review specific decisions.

[65] Lawrence M Rause, "High-Tech Industries Drive Global Economic Activity," National Science Foundation NSF 98-313 (July 20, 1998)
[66] Bradley K. Steinbrecher, "THE IMPACT OF THE CLINTON ADMINISTRATION'S EXPORT PROMOTION PLAN ON U.S. EXPORTS OF COMPUTERS AND HIGH-TECHNOLOGY EQUIPMENT," *U. Pa. J. Int'l Bus. L.*, vol. 15, n. 4, 1995, 675.
[67] Mark D. Gursky, "Liberalization of High Performance Computer Export Controls under the Clinton Administration: Balancing National Security and Economic Interests," 49 Cath. U. L. Rev. 975 (2000), 991.

For added protection, though, BIS began to publish a list of specific "entities" in various countries (individuals, businesses, institutions, and organizations) – e.g. individual end customers who would be subject to extra-rigorous licensing requirements on top of existing dual-use export controls applied to their country. When the Entity List was initially published in 1997, the purpose was to identify entities based solely on whether their activities "could result in an increased risk of the diversion of exported, reexported, and transferred items… to…WMD programs."[68] In subsequent iterations of the Entity List, grounds for inclusion expanded to include unspecified "other activities contrary to U.S. national security and/or foreign policy interests."[69]

After becoming Clinton's Defense Secretary, Perry established an official policy of increasing reliance on dual-use technologies as a way to advance U.S. military capabilities despite Congressional pressure to lower defense spending.[70] Much of the United States' huge post-Cold War military advantage leveraged space and digital technologies developed by the private sector to enhance global reconnaissance and precision strike capabilities, key elements of what was called the Revolution in Military Affairs (RMA). The expectation in the 1990s was that rapid expansion in the global commercial space and IT sectors would incentivize entrepreneurs to innovate, increase efficiency, and provide economies of scale. The U.S. military could get better products, more quickly by purchasing "off the shelf" rather than investing its own money in research, development, and production of customized military goods.

Further cost-savings for the public and private sectors could be achieved through close cooperation with Russia on civilian space activities, and use of low-cost Chinese launch services for commercial satellites. Defense Secretary Perry, Joint Chiefs of Staff Vice-Chairman William Owens, and other leading defense intellectuals were less concerned in the 1990s about what countries like Russia and China would do with advanced dual-use technologies and products than they had been during the Cold War because they now viewed those countries as partners in efforts to prevent proliferation. They maintained that as long as the United States used its intelligence and force projection capabilities to solve global security problems in ways that other major powers liked, they would be happy to reap more economic benefits by focusing on commercial and civilian applications of dual-use technologies that were increasingly available at more affordable prices.[71]

The Clinton administration pursued some *cooperative management* initiatives, without completely replacing secrecy and access-denial mechanisms. The Wassenaar Arrangement, COCOM's successor, relied on consultation and coordination among dual-use technology suppliers to prevent the most worrisome forms of proliferation without impeding mutually beneficial trade. While the Russian Federation and some Eastern European countries joined the new group, other major arms exporters, including China and Israel, did not. The Wassenaar

[68] "Entity List" Bureau of Industry and Security, U.S. Department of Commerce, accessed Jan 17, 2023, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.
[69] "Lists of Parties of Concern," Bureau of Industry and Security, U.S. Department of Commerce, accessed Jan 17, 2023, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern.
[70] Reppy, "Managing Dual-Use Technology in an Age of Uncertainty," 3.
[71] Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs* (March/April 1996).

Arrangement emphasizes transparency, information exchange, and harmonization of national trade control decisions about what is too dangerous or destabilizing to sell to any non-Wassenaar member, rather than multilateral agreement not to transfer certain items to specific countries of concern. Members are encouraged to exercise "extreme vigilance" regarding transfers of some very sensitive items, such as stealth technology and radars. They are expected to report regularly on export licenses approved or denied to non-Wassenaar members. They are also requested to report when they approve transactions that are "essentially identical" to transactions denied by other members, although countries cannot veto other members' technology transfers.[72]

The United States also worked with former Soviet Union and Eastern bloc countries, China, and eventually other states, on cooperative threat reduction projects intended to help recipients build export control capacity. For example, the State Department established the Export Control and Related Border Security Program (EXBS) to prevent WMD proliferation and excess accumulation of conventional weapons. Over time, the program expanded to new geographies and, in 2020, maintained a $64.9 million budget to carry out training, exchanges, interagency coordination, and implementation support with supplier countries and countries in possession of sensitive materials.[73]

The Clinton administration was particularly concerned about nuclear and ballistic missile proliferation in South Asia, but U.S. efforts to deny India the necessary technology backfired. When India decided in the early 1980s to complement its space program with a dedicated ballistic missile program, it anticipated new constraints on dual-use technologies for those programs, as had occurred after India's nuclear test, and made a concerted effort to develop indigenous capabilities.[74] In 1993, India tried to buy cryogenic rocket engines and advanced technology for satellite launch vehicles from Russia, but the United States threatened to withhold financial assistance and impose sanctions on Russian defense companies because the technology could also be used to improve India's nascent ballistic missile program. This attempt at coercive economic statecraft increased Russian suspicions about U.S. motives for helping Russia after the Soviet Union collapsed. Moscow accused the United States of trying to minimize competition in the lucrative space launch industry, and hypocritically allowing its own companies to compensate for lower defense spending by selling supercomputers to China that could be used for nuclear weapons development. Russia eventually compromised by dropping the formal tech transfer part of the deal and joining the MTCR in return for contracts to launch U.S. satellites and participation in the International Space Station project.[75]

MTCR constraints slowed, but did not stop, Indian ballistic missile development in response to China's nuclear and missile capabilities. India's first flight tested its Prithvi 1 short-range (150

[72] The Arms Control Association, "The Wassenaar Arrangement at a Glance," (last updated February 2022) at: https://www.armscontrol.org/factsheets/wassenaar.
[73] For summary, see, "The EXBS Program," *A Resource on Strategic Trade Management and Export Controls*, https://2009-2017.state.gov/strategictrade/program/index.htm# and https://www.state.gov/wp-content/uploads/2019/05/FY-2020-CBJ-FINAL.pdf
[74] Waheguru Pal Singh Sidhu, "Looking Back: The Missile Technology Control Regime," *Arms Control Today* (April 2007).
[75] Daniel R. Kempton and Roni Du Preez, "Up in Arms: Russia's Sale of Cryogenic Rocket Engines to India," Case 228, Georgetown Institute for the Study of Diplomacy (2000).

km) ballistic missile in 1988 and the Agni 1 (700 km range) ballistic missile in 1989, soon after the MTCR was established. Dinshaw Mistry estimates that indigenous development of key components for India's ballistic missile program took five extra years and increased costs by 10% compared to purchasing them from a foreign supplier,[76] but perceived discrimination in technology transfer policies bred Indian resentment. Prime Minister Rao faced domestic opposition for suspending missile tests for several years, in response to calls for restraint from the United States and technological problems.[77] Criticism from Indian nationalists intensified in response to diplomatic pressure on India to sign the 1996 Comprehensive Nuclear Test Ban Treaty. That contributed to the election of a Hindu nationalist prime minister who conducted an overt nuclear weapon test in 1998. In response, the United States added several hundred institutions, including "all of the crown jewels of India's 'strategic enclave'," to the BIS list of entities subject to extra-tight restrictions on dual-use technology transfers.[78] By then, though, India had all the technology it needed to test the Agni II, a medium-range solid-fueled missile capable of carrying nuclear warheads over a 2000 km range in April 1999.

Export controls and U.S. pressure for restraint also delayed, but did not stop, Pakistan's efforts to acquire its own nuclear warheads and ballistic missiles in response to India's achievements. Pakistan first tested short-range ballistic missiles in 1989, shortly after India's first Prithvi missile test. The United States imposed nonproliferation sanctions on Pakistan the following year, but it continued to receive some missile transfers and technological assistance from China and North Korea to supplement its indigenous development efforts. The United States also proposed a bilateral South Asian missile control initiative; Pakistan responded favorably, but India refused because China was not included. Pakistan continued to develop two medium-range ballistic missiles, but did not test them until after India began deploying Prithvi I missiles in 1997. Under domestic pressure to respond, Pakistan first tested the Ghauri-1 liquid-fueled missile (1,000 km) in 1998, the Shaheen I solid-fueled missile (600-800 km) in 1999, and the Shaheen-2 (1,500-2,000 km) in 2004. Mistry argues that technical assistance from China and North Korea shortened the time for Pakistan to test these missiles by a few years, but that it had enough indigenous capability that it could have eventually built these systems even if all foreign suppliers had fully joined the technology blockade.[79]

If export controls can delay, but rarely permanently deny technology acquisition by a highly motivated country, whether the longer-term security value of those controls outweighs their costs depends on how the extra time they provide is used. Clinton administration efforts to reduce the economic and political costs of excessive export controls helped make the net effect more positive in the 1990s. U.S. high tech industries regained much of the global market share lost over the previous decade,[80] and by 1996, the percentage of U.S. GDP from trade was up to 8.7%, about what it had been before Reagan took office. Increased trade and technology collaboration with countries like Russia and China improved political relations with key countries, and helped

[76] Mistry, *Containing Missile Proliferation,* p. 116.
[77] Mistry, *Containing Missile Proliferation,* p. 117.
[78] Ashley Tellis, "The Evolution of U.S.-Indian Ties: Missile Defense in and Emerging Strategic Relationship," *International Security* 30:4 (Spring 2006) 124-5.
[79] Mistry, *Containing Missile Proliferation,* p. 116.
[80] Rausch, "High-Tech Industries Drive Global Economic Activity."

advance some non-proliferation objectives, such as persuading a number of countries to join the MTCR and convincing China to better align its export practices with MTCR guidelines.[81] Most NNWS that joined the MTCR agreed to eliminate their offensive missiles and associated equipment as a condition of entry, while the United States and Russia destroyed more than 5,000 long and intermediate-range ballistic and cruise missiles to implement the 1987 Intermediate-range Nuclear Forces treaty and the two Strategic Arms Reduction Treaties (1991 and 1993). These actions complemented supply side measures and changed the normative and security context in ways that help explain why a number of countries that successfully developed short- and medium-range ballistic missiles did not deploy them in large numbers, and did not make a similarly determined effort to develop longer-range ballistic missiles during this time.

The United States also hedged against the global spread of advanced technologies by using the economic gains from trade to accelerate its own military innovation. One study suggested that since proliferation of space-based capabilities that gave the United States military and economy its "information edge" was inevitable, the Clinton administration could avoid hegemonic decline by selling enough high-tech goods and services to keep capital flowing into those industries, enabling them to innovate fast enough to maintain U.S. military and economic superiority. It showed that relaxing restrictions on foreign sales of three types of dual-use space technologies – satellite-based remote sensing, communications satellites, and high-accuracy data from global positioning and navigation satellites – helped generate sufficient revenue and spur enough innovation for the United States to improve its protection against any negative effects of proliferation.[82]

The end of the Cold War had reduced, but did not eliminate, concerns about how increased trade and scientific cooperation might empower Russia and China for future strategic competition. Congressional critics attacked Clinton's cooperative security, technology transfer, and export control policies as naively helping Russia to get back on its feet and China to gain capabilities needed to become a peer competitor. For example, after Chinese launch vehicles exploded in 1995 and 1996, killing people and destroying expensive U.S. communication satellites, Commerce allowed their owners, Hughes Electronics Corporation and Loral Space & Communications, to share sensitive technical data with the Chinese for launch failure investigations.[83] Members of Congress were outraged after intelligence reviews found that the information could also be used to improve Chinese ballistic missiles.[84] The Republican-controlled Congress subsequently used an amendment to the 1999 Defense appropriations bill to put space satellites back under the tighter purview of the State Department, foreshadowing efforts by the next administration to take a more coercive approach to export controls. To be on the safe side, the State Department also revoked Commerce's determination that some basic items, like screws, did not require export licenses, and unilaterally extended all satellite-related

[81] Victor Zaborsky, "Does China Belong in the MTCR?" *Arms Control Today* (October 2004).
[82] Derek D. Smith, "A Double-Edged Sword: Controlling the Proliferation of Dual-Use Satellite Systems," *National Security Studies Quarterly* VII:2 (Spring 2001, 31-68.
[83] John Mintz, "Missile Failures led to Loral-China Link, *The Washington Post, June 12, 1998.*
[84] "China: Possible Missile Technology Transfers Under U.S. Satellite Export Policy -- Actions and Chronology," Congressional Research Service, August 1998, 7.

controls even to allies.[85] These moves frustrated the U.S. commercial space industry and prospective customers in allied countries while motivating China to build up its own space expertise to reduce its reliance on the United States in this field.

Coercive prevention to counter WMD proliferation

The George W. Bush administration saw more dangers in the post-Cold War world than its predecessor did. It shared the Clinton administration's concern that relatively weak rogue states could use WMD to attack major powers. It considered that threat more imminent, though, based on the assessment of a 1998 commission led by Secretary of Defense Donald Rumsfeld that North Korea, Iran, and other states could have ballistic missiles capable of hitting the United States within a few years if they got foreign assistance.[86] The September 11, 2001 terrorist attacks and subsequent anthrax letters added a new focus on preventing nonstate actors from accessing nuclear, biological, and chemical weapons and the means to make them. At the same time, Bush officials' realpolitik worldview fueled expectations that a resurgent Russia and a rising China would eventually challenge U.S. dominance unless the United States substantially increased investments in transformative military capabilities.

Bush officials believed that as the sole military, economic, and technological superpower in a dangerous and uncertain world, the United States could and should prioritize unilateral security strategies. The "global war on terror" made no distinction of accountability between terrorists and rogue nations that might harbor or help them.[87] The 2002 State of the Union address described Iran, Iraq, and North Korea as an "axis of evil" that could provide terrorists with means to inflict catastrophic harm on the United States and its allies.[88] The 2002 NSS depicted these adversaries as much less deterrable than the Soviet Union had been. Therefore, the United States needed a much more proactive strategy, including preventive military strikes on facilities that might contain WMD-related technologies, preemptive action to destroy WMD before they could be used, and missile defense to intercept in-coming ballistic weapons.

The Bush administration invested heavily in leveraging U.S. technological advantages to transform its military capabilities for the twenty-first century in the belief that innovation, entrepreneurial ingenuity, and high defense spending could perpetually ensure that the United States remained ahead of all potential challengers. It reconfigured the Cold War nuclear triad to become a post-Cold War strategic triad composed of nuclear and conventional offensive weapons, layered missile defenses, and a "responsive infrastructure" that could rapidly manufacture additional military capabilities. Whereas Clinton defense officials like Perry and Owens sought RMA capabilities so the United States military could perform unique functions for

[85] Howard Diamond, "Congress Returns Export Control Over Satellites to State Department," *Arms Control Today*, (October 1998).
[86] "Executive Summary of the Report of the Commission to Assess the Ballistic Missile Threat to the United States," The Honorable Donald H. Rumsfeld, Chairman (July 15, 1998), at: https://irp.fas.org/threat/bm-threat.htm.
[87] George W. Bush, Decision Points (New York: Broadway Paperbacks, 2010), 396.
[88] "President Delivers the State of the Union Address," President George W. Bush White House archived website, Jan. 29, 2002, https://georgewbush-whitehouse.archives.gov/news/releases/2002/01/20020129-11.html

global cooperative security operations, the Bush administration's RMA envisioned integrating advanced sensors, communications, and computing capabilities into a prompt global strike capability capable of finding, tracking, targeting, and destroying threats located anywhere on earth or in space within an hour of an order to do so. It also hoped these digital technologies could overcome long-standing problems like counter-measure discrimination that had previously precluded deploying more than a very rudimentary missile defense system.

The Bush administration continued its predecessor's practice of saving money by purchasing many of the components for RMA weapons systems from U.S. and foreign companies that got economies of scale by selling to a variety of customers in many different countries. Judith Reppy noted that fielding transformative military capabilities built from commercial technology was risky. It deepened dependence on foreign suppliers for critical components, and showed other countries' militaries how they, too, could acquire advanced capabilities faster, better, and cheaper, thus potentially eroding U.S. military superiority. The United States was the clear leader in RMA applications of information and space technologies, and Reppy predicted it would remain so indefinitely because of comparatively high investment by the U.S. government. Yet, "that very investment promotes rapid technological change and thus exacerbates the problem of keeping control lists up to date." If they covered entire categories of emerging technologies, they would be difficult to administer, harm U.S. economic interests, and breed resentment abroad. If they were too narrow, though, they would inevitably leave out dual-use technologies that could have important military applications. She concluded that "RMA technologies are a textbook example of the problems facing those who would manage technology to enhance security while promoting dual-use applications."[89]

The United States and some allies began revealing sensitive intelligence information to build support for implementing a unilateral militarized counter-proliferation strategy. In October 2002, senior State Department officials publicly asserted that North Korea, after being confronted with damning U.S. intelligence, had admitted to having a secret uranium enrichment program not covered by the 1994 Agreed Framework, ending that diplomatic effort to address international concerns about North Korea's nuclear program.[90] The following February, Secretary of State Colin Powell laid the groundwork for the U.S. invasion of Iraq by presenting evidence that Iraq was reconstituting banned WMD programs, much of which was later discredited. Three months later, an external group of Iranians seeking the overthrow of the current regime publicized intelligence indicating that Iran was building a uranium enrichment facility that it had not declared to the IAEA.[91] Efforts by the IAEA and the EU3 (Britain, France, and Germany) made progress toward a diplomatic resolution that would have kept the Iranian nuclear program more tightly constrained than the agreement reached in 2015 did, but the United States objected to any arrangement allowing Iran even a token enrichment capability. In 2004, Pakistani scientist A.Q.

[89] Reppy, "Managing Dual-Use Technology in an Age of Uncertainty," 7. On this point, see also Stephen G. Brooks, *Producing Security: Multinational Corporations, Globalization, & the Changing Calculus of Conflict* (Princeton University Press, 2005).
[90] Paul Kerr, "North Korea Admits Secret Nuclear Weapons Program," *Arms Control Today* (November 2002).
[91] NNWS subject to IAEA safeguards are obligated to report the construction of such facilities six months before bringing nuclear material on site, a milestone that Iran had not yet reached. This revelation was used as clear-cut evidence that Iran had a clandestine nuclear weapons development program when most of the intelligence supporting that judgment was classified.

Khan confessed under pressure that he had evaded export controls for years to illicitly transfer nuclear technology and material to countries like Iran, North Korea and Libya, underscoring the growing danger posed by "proliferation rings" – e.g., networks through which proliferating states and private sector actors would help each other acquire nuclear weapons and ballistic missiles more quickly and efficiently than any developing country could do on its own.

Although speeches and policy documents routinely depicted U.S. efforts to deploy missile defenses, develop prompt global strike weapons, and achieve comprehensive space dominance as driven by WMD counterproliferation and the global war on terror, Russia and China speculated that the United States also had other motives. They questioned why the United States, which was already spending roughly the same amount on its military in 2001 as the other nine top spenders combined ($281.4 billion)[92], would more than double that figure to $661 billion by 2009, unless it was preparing to fight a future peer competitor.[93] They also maintained that if the United States really only wanted a limited missile defense and a niche prompt global strike force sized to neutralize the small threat from a proliferator's nascent arsenal, Bush officials would not be so adamantly opposed to arms control. To hedge against the possibility that U.S. advances in strategic offense and defense might erode the deterrent value of China's small nuclear arsenal, or Russia's much larger one, those two countries intensified efforts to emulate or offset U.S. military uses of advanced technologies. Even as the United States struggled militarily in Iraq and Afghanistan, the 2006 NSG expressed growing concern about Russia and China. It also mentioned a new "disruptive" category of security challenge involving "state and nonstate actors who employ technologies and capabilities (such as biotechnology, cyber and space operations, or directed-energy weapons) in new ways to counter military advantages the United States currently enjoys."[94]

Bush officials tightened U.S. export controls, with predictable negative effects. The value of exported goods and services as a share of the U.S. GDP dropped from 10.7% in 2000 to 10% in 2005 while the global average continued to rise sharply, from 23.6% in 2000 to 27.2% in 2005.[95] Strict controls on commercial satellites reduced U.S. market share from 80% in the 1990s to 50% by 2006. China purchased six satellites from European and Israeli suppliers in the early 2000s – an estimated loss between $1.5 to 3.0 billion for the U.S. economy. It also developed an indigenous communications satellite, which it successfully launched in 2008, and started selling to other countries impacted by U.S. export controls.[96] The two main U.S. satellite manufacturing and launch companies, Boeing and Lockheed Martin, used the Satellite Industry Association to complain about the burdens of export controls, but treaded carefully because they depended on military contracts to make up for commercial revenue that failed to materialize after the telecom bubble burst in the late 1990s. The Bush administration tried to leverage space launch cooperation to dissuade Russia from missile-related trade with Iran, but backed off when it

[92] "Military expenditure," Chapter 6 in *SIPRI Yearbook 2002: Armaments, Disarmament and International Security*, pp. 235.
[93] Sam Perlo-Freeman, Olawale Ismail, and Carina Solmirano, "Military Expenditure," Chapter 5 in *SIPRI Yearbook 2010*, pp. 11.
[94] "National Security Strategy of the United States," (March 2006,) p. 44. https://georgewbush-whitehouse.archives.gov/nsc/nss/2006/.
[95] Data.worldbank.org.
[96] Ray Zelnio, "The Effects of Export Control on the Space Industry," *The Space Review* (January 16, 2006).

realized that Boeing and Lockheed-Martin used Russian-made hardware.[97] These difficulties balancing security, economic, technology, and foreign policy considerations led Bush to initiate a dual-use export control reform process in 2008, but it made little progress before he left office.[98]

The Bush administration supplemented the unilateral aspects of its security strategy with voluntary cooperation with like-minded states to deny dangerous dual-use capabilities to untrustworthy countries and nonstate actors, a variation on the *suppliers against seekers* approach. The more countries, companies, and other types of entities whose participation is necessary for effective controls, the harder it is to get agreement on legally binding rules with effective verification and enforcement mechanisms. Therefore, Bush officials justified their preference for informal, voluntary arrangements as a way to avoid time-consuming negotiations, and "cumbersome treaty-based bureaucracies."[99] But noninstitutionalized coordination also served the Bush administration's desire to loosen legally binding international constraints not only on U.S. military activities, as in its 2002 withdrawal from the Antiballistic Missile Treaty, but also on its freedom to decide when the economic and political benefits of selling WMD-related technologies to a particular country outweighed the risk to global security.

The one significant legally binding multilateral initiative taken by the Bush administration in this sphere was UN Security Council Resolution 1540, adopted in 2004 under Chapter VII of the UN Charter. It prohibited UN member states from providing any form of support to nonstate actors who might be trying to acquire nuclear, biological, and chemical weapons. It also mandated that they develop, implement, and report on comprehensive national regulatory systems for tracking and securing the production, distribution, and financing of WMD-related technologies and services.[100] In contrast to national regulatory rules and multilateral nonproliferation treaties, where sovereign states decide for themselves what obligations to take on, United Nations Security Council Resolution (UNSCR) 1540 was imposed on all UN member states by the Security Council. In keeping with the Bush administration's antipathy toward international bureaucracies, though, the resolution did not establish a standing implementation body, like the Organization for the Prevention of Chemical Weapons, or any independent verification arrangements to supplement self-reporting, giving member states a lot of leeway to interpret or ignore its mandates.

Many UN members initially resented the unusual means by which this legal obligation was imposed on them without their consent, and were slow to start carrying out its regulatory requirements. Since the United States had justified invading Iraq in 2003 as enforcement of earlier Security Council resolutions, some countries also worried that UNSCR 1540 could become a pre-approved basis for invasion of other suspected proliferators with ties to terrorist organizations. Skepticism decreased over time because the Security Council emphasized voluntary cooperation over coercive enforcement, with the United States at the forefront of

[97] Amy Svitak, "U.S. Backs off Scrutiny of Russian Exports," *DefenseNews* March 10, 2003.
[98] National Security Presidential Directive 55, January 22, 2008, https://fas.org/irp/offdocs/nspd/nspd-55.pdf
[99] "An All-Out War on Proliferation," Financial Times op-ed by John Bolton, September 7, 2004, https://2001-2009.state.gov/t/us/rm/36035.htm
[100] https://www.un.org/disarmament/wmd/sc1540/

countries providing capacity-building services for those who requested help meeting their UNSCR 1540 obligations. By 2011, over 120 countries had nuclear, chemical, and biological weapons-related strategic trade control legislation and enforcement mechanisms in place, an achievement that would not have been possible without the NPT, the Chemical Weapons Convention, the Biological Weapons Convention, and other foundational treaties and regimes to "provide structural integrity to the normative foundations of the [UNSCR 1540] regime."[101]

UNSCR 1540 increased multilateral efforts to supplement export controls with international information-sharing about financing for proliferation-related activities, a basic version of what Reinecke had recommended. The United States and other G-7 countries had formed the Financial Action Task Force in the late 1980s to combat money laundering, then expanded both its membership and its mandate after the Cold War ended. Financial institutions began sharing information about suspicious transactions to identify drug trafficking and terrorist operations, as well as proliferation rings like the A.Q. Khan network. Proliferators took advantage of global commerce to purchase WMD-relevant dual use items in countries with lax export controls. The hope, therefore, was that illicit transactions relying on intermediaries and front companies could be identified by suspicious payments flowing through global financial institutions that were based outside the jurisdiction of the country where the physical sale of the dual-use item had occurred.[102] In practice, though, it has proven more difficult for financial institutions to implement country-specific and general anti-proliferation controls than to use these tools against money laundering, drug trafficking, and terrorist operations.[103]

The Proliferation Security Initiative (PSI) exemplified the purely voluntary, informal approach to security cooperation that the Bush administration generally preferred. Launched in May 2003, the PSI aimed to increase interdiction of weapons and materials of mass destruction by sharing information and improving coordination with like-minded countries. The Bush administration underscored that it was "an activity, not an organization."[104] Ten countries – Australia, France, Germany, Italy, Japan, the Netherlands, Poland, Portugal, Spain, and the United Kingdom – initially endorsed the PSI's statement of principles, thereby indicating their intention to utilize national laws and bilateral boarding agreements to interdict ships carrying potentially dangerous cargo when they passed through water under the signatories' jurisdiction. As of 2019, 107 countries, including Russia, have endorsed the PSI's statement of principles, which each

[101] Brian R. Early, Mark T. Nance, and M. Patrick Cottrell, "Global governance at the energy-security nexus: Lessons from UNSCR 1540," *Energy Research and Social Science* 24 (2017), 94-101.
[102] Financial Action Task Force Committee Project Team on Proliferation Financing, "Combating Proliferation Financing: A Status Report on Policy Development and Consultation," (February 2010), at: http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.
[103] Togzhan Kassenova, "Challenges Implementing Proliferation Financing Controls: How Export Controls can Help," *World ECR: The Journal of Export Controls and Sanctions* (May 30, 2018).
[104] Susan J Koch, "Proliferation Security Initiative: Origins and Evolution," Occasional Paper No. 9, National Defense University Center for the Study of Weapons of Mass Destruction (June 2012).

interprets as it sees fit.[105] China remains notably absent from that list, viewing the initiative as an attempt to replace existing multilateral efforts and target specific countries like North Korea.[106]

While pressing other countries to deny hostile states and nonstate actors access to dangerous dual-use technologies, the Bush administration loosened unilateral and multilateral export controls on India for strategic, economic, and domestic political reasons. Soon after taking office, it began trying to overcome India's long-standing opposition to missile defense by promising "breathtaking" technological cooperation for countries willing to support the Bush administration's plans to move from threats of mutual assured destruction and legally binding bilateral arms control to a security system based on U.S. conventional military superiority, missile defense, and voluntary cooperation.[107] In 2005, the United States and India formed a strategic partnership "to counter terrorism relentlessly" and " to create an international environment conducive to the promotion of democratic values." This bilateral move involved *allies versus adversaries* transfers of dual-use technologies intended to align India with regional coalitions the Bush administration was building to counter China's growing power, but it had unintended negative effects on multilateral nonproliferation mechanisms.[108]

The part of this new strategic partnership that got the most attention involved the United States changing long-standing nonproliferation policy, U.S. law, and NSG practices to facilitate peaceful nuclear trade with India even though it had never signed the NPT and had a growing nuclear arsenal. U.S. arguments for treating India as an exception to NPT and NSG rules for dual-use nuclear cooperation created openings for Russia, China, Pakistan, Israel, and others to grant or seek their own exceptions to the global rules, often in ways that U.S. officials saw as increasing nuclear proliferation risks.[109] Equally important were U.S. pledges to engage with India on various forms of space and missile cooperation. This necessitated U.S. reinterpretation of the MTCR guidelines to apply only to "offensive" missiles, not those intended for defensive missions, even though the latter could be used to shoot down satellites more easily than ballistic missiles. India did precisely that in 2019, becoming the fourth country to demonstrate its mastery of hit-to-kill anti-satellite (ASAT) technology.[110]

In short, the Bush administration's approach of tightening or loosening restrictions on dual-use technologies depending on the nature of U.S. relations with a given country, made a hard problem worse in several ways. By unilaterally deciding that Iran should not be allowed to have any nuclear enrichment capabilities regardless of what IAEA safeguards it was willing to accept, while India should get an exemption from the NSG requirement that all recipient countries must

[105] Arms Control Association, "The Proliferation Security Initiative (PSI) at a Glance," Last updated in March 2020, https://www.armscontrol.org/factsheets/PSI
[106] See, for example, Ministry of Affairs of the People's Republic of China, "The Proliferation Security Initiative," April 7, 2011, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/fkswt_665240/200802/t20080229_599805.html
[107] Tellis, 133.
[108] See, Joint Statement by President George W. Bush and Prime Minister Manmohan Singh, https://2001-2009.state.gov/p/sca/rls/pr/2005/49763.htm
[109] Sharon Squassoni, "The U.S.-India Nuclear Deal and Its Impact," *Arms Control Today* (July 2010).
[110] Kelsey Davenport, "Indian ASAT Test Raises Space Risks," *Arms Control Today* (May 2019).

have comprehensive IAEA safeguards covering their entire nuclear program, the Bush administration weakened support for long-standing multilateral arrangements like the NPT and the NSG. It used U.S. leadership to promote less institutionalized non-proliferation tools such as UNSCR 1540 and PSI that lacked clear rules, effective verification, and authoritative compliance mechanisms. At the same time, many of the Bush administration's security policies and military programs made countries outside the U.S. alliance system feel threatened, increasing their incentives to invest in indigenous development of dual-use technologies and find other ways to circumvent denial-based control strategies. As we have shown, foreign demand rose both for WMD-related dual-use capabilities that were the current focus of national and multilateral control efforts, and for digital, space and other RMA-related technologies, many of which were not subject to strategic trade controls. This confirmed predictions from the early 1990s that protections against the deliberate or inadvertent misuse of WMD-related technologies would not keep pace with the size and complexity of the growing challenge unless suppliers and seekers engaged more extensive forms of cooperative management than anything pursued by the Clinton administration. The growing inadequacies of preventive controls might have been acceptable if the Bush administration had been able to use very high rates of military spending and even larger private sector investments in technological innovation to provide offensive and defensive capabilities that could neutralize whatever threatening capabilities its rivals managed to acquire. But the United States never achieved that goal even at the height of its post-Cold War military, economic and technological dominance, in part because the "disarray" in Bush administration policies to control the spread of military-related technology eroded all three areas of leadership.[111]

Entering a new era of strategic trade controls on emerging technologies?

If the most fundamental question about governance of dual-use technologies during the 1990s and early 2000s was whether cooperative management or coercive denial was better able to prevent WMD proliferation without unduly harming economic growth and technological innovation, an even more basic question emerged during the Obama administration that remains unanswered. What is the main security problem that strategic trade controls are meant to address? While some Obama officials were trying to make domestic and international controls against WMD proliferation more effective and efficient, others were raising alarms about the dangers posed by a broad collection of "emerging" technologies, particularly as they might be used against the United States in a new era of great power competition. During the Trump administration, a broad bipartisan consensus formed around the desirability of strengthening strategic trade controls on emerging technologies to (re-)gain advantage in great power competition with China. As we will show, though, there is little agreement among key U.S. stakeholders, let alone between the United States and its allies, about what specifically should be controlled, why that was desirable, and how it should be done. Moreover, the U.S. government is even less capable now than before of instituting effective controls without full cooperation from private industry, academia, allies, and other technologically advanced countries – important

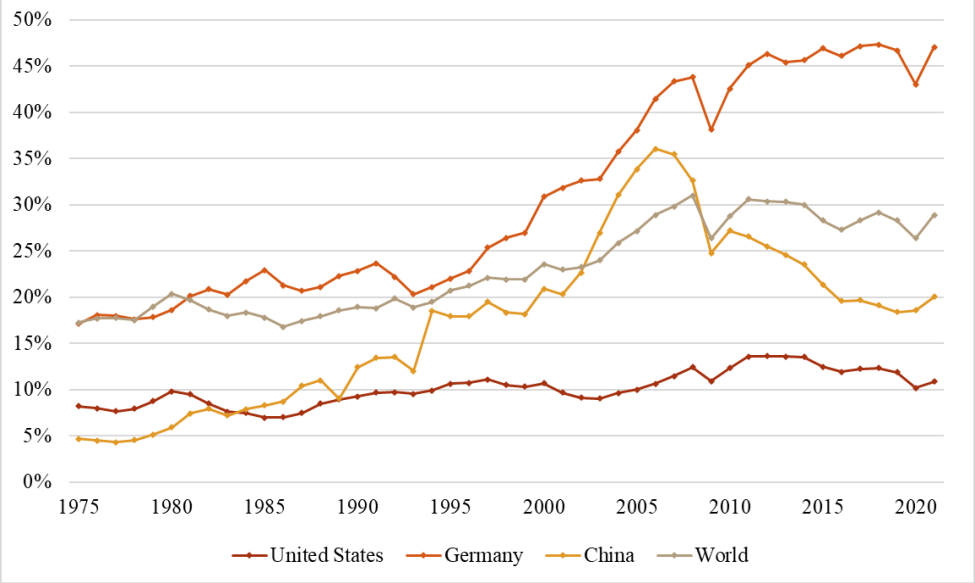
[111] Reppy, p. 2.

stakeholders with very different ideas about how to balance security, economics, and foreign policy objectives.

Obama efforts to simplify U.S. export control system as security problems grow more complex

Soon after taking office, President Barack Obama launched a major overhaul of the nation's export control system that critics believed had become too broad, strict, and time-consuming for a highly connected information-age global economy fueled by rapid digital innovation.[112] From the early 1990s through the mid-2000s, the contributions made by exports of goods and services to GDP in countries like Germany and China had increased dramatically, while remaining essentially flat for the United States (see Figure 2). The percentage of U.S. exports involving high technology goods,[113] rather than other manufactured goods, began to drop dramatically during the Bush administration, while remaining relatively stable for China and Germany (see Figure 3). By the early Obama years, the United States had less market share and influence in critical high-tech sectors than it had during the Cold War or in the period of post-Cold War U.S. global dominance. Another motivation for export control reform was that by 2009, technologies originating in the private sector had overtaken those that were attributed to the government in both quantity and quality.

Figure 2. Exports of Goods and Services (% of GDP), 1975 – 2021

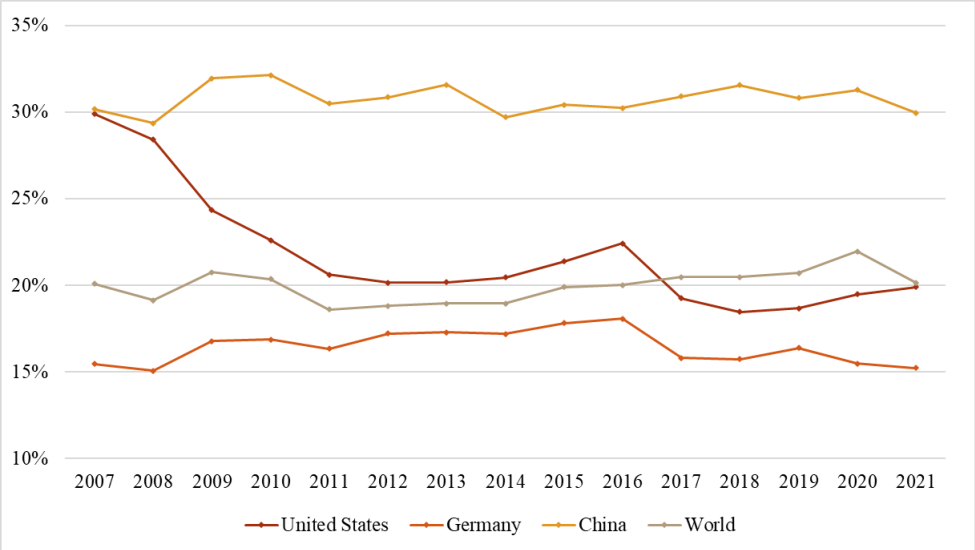


Source: World Bank national accounts data, and OECD National Accounts data files.

[112] Andrea Stricker and David Albright, "U.S Export Control Reform: Impacts and Implications for Controlling the Exports of Proliferation-Sensitive Goods and Technologies, A Policy Document for the New President and Congress," Institute for Science and International Security, May 17, 2017, https://isis-online.org/isis-reports/detail/u.s.-export-control-reform-impacts-and-implications/, p.6

[113] The World Bank defines high-technology exports as "products with high R&D intensity, such as in aerospace, computers, pharmaceuticals, scientific instruments, and electrical machinery," From: Metadata Glossary, World Bank, Accessed January 18, 2023, https://databank.worldbank.org/metadataglossary/world-development-indicators/series/TX.MNF.TECH.ZS.UN.

Figure 3. High Technology Exports (% of Manufactured Exports), 2007 - 2021



Source: World Bank national accounts data, and OECD National Accounts data files.

Like previous reform efforts, the Export Control Reform Initiative sought to increase U.S. economic competitiveness without damaging U.S. security by building "higher walls" around the most sensitive technologies while loosening restrictions for less sensitive items.[114] The most innovative aspect of this reform initiative was to simplify the export control system and reduce bureaucratic burdens by creating four "singles:" a single licensing agency to handle both dual-use items and munitions, a single commodities list, a single enforcement coordination agency and a single information technology platform that combined multiple databases.[115] The administration made progress, but could not get Congressional approval to consolidate responsibility for export licenses.[116]

The most significant change involved the transfer of thousands of goods from the strictly-regulated USML under the International Traffic in Arms Regulations, administered by the State Department's Directorate of Defense Trade Controls, to the more flexible CCL under the Export Administration Regulations, administered by BIS. That change drew mixed reviews, with advocates saying that it cut red tape and allowed officials to focus their attention on fewer items,

[114] "President Obama Lays the Foundations for a New Export Control System to Strengthen National Security and the Competitiveness of Key U.S. Manufacturing and Technology Sectors," The White House Office of the Secretary archived website, August 30, 2010 https://obamawhitehouse.archives.gov/the-press-office/2010/08/30/president-obama-lays-foundation-a-new-export-control-system-strengthen-n,
[115] Zach Weinberg, "Reforming U.S. Export Controls to Reflect the Threat Landscape," Journal of Public & International Affairs, May 5, 2021, https://jpia.princeton.edu/news/reforming-us-export-controls-reflect-threat-landscape and Department of Defense, Remarks by Secretary Gates to the Business Executives for National Security on the U.S. Export Control System, April 20, 2010, https://sgp.fas.org/news/2010/04/gates-export.html
[116] Stricker and Albright, "U.S Export Control Reform: Impacts and Implications for Controlling the Exports of Proliferation-Sensitive Goods and Technologies, A Policy Document for the New President and Congress," p.10

and critics saying that it harmed nonproliferation efforts by making it easier for adversaries to obtain sensitive items.[117]

This export control reform process began in the context of a larger Obama administration effort to undo some of the most unilateral and unpopular aspects of the Bush administration's international security policies. President Obama's 2009 speech in Prague called on world leaders to join him in a concerted effort to eliminate nuclear weapons, through further reductions with Russia, re-invigorated nonproliferation diplomacy, and Nuclear Security Summits to prevent catastrophic terrorism.[118] He tried to strengthen and institutionalize multilateral nonproliferation initiatives from the Bush years, such as the UNSCR 1540 Committee and the PSI. His administration also proposed, and in some cases agreed with Russia and China on voluntary transparency and confidence-building measures to reduce risks associated with cyber and space activities, such as establishing communication procedures to discuss worrisome incidents in these spheres. At the same time, the Obama administration continued some versions of many Bush-era security programs that Russia and China considered particularly threatening, including missile defense, and dramatically expanded some high-tech programs that blurred the lines between war and peace, such as using armed drones for counter-terrorism operations. The grueling battle for New START ratification and opposition even from some Democratic members of Congress to any agreement with Iran that did not permanently end all dual-use nuclear activities also caused foreign leaders to question whether Obama was really all that different from Bush.

Prospects for cooperation with Russia and China were further complicated during Obama's second term in office by China's assertive behavior regarding contested territorial claims and Russia's 2014 annexation of Crimea from Ukraine. By 2014, some members of the DOD and the intelligence community had come to see China and Russia as current strategic competitors, rather than potential future threats as the previous administration did.[119] The official Obama administration position expressed increased concern, but still refrained from labeling them adversaries. It continued to cooperate with them in negotiations over Iran's nuclear program and other multilateral efforts to keep WMD-related capabilities away from potential proliferators and terrorist groups.[120]

Concerns that China might soon threaten U.S. technological superiority were reinforced when the Chinese government announced a comprehensive 10-year plan to upgrade Chinese technology development and manufacturing so Chinese firms could cooperate on more equal terms and compete more effectively with other advanced industrialized countries.[121] Some in U.S. policy circles interpreted the Made in China 2025 blueprint (MIC 2025) as top-down guidance to gain strategic advantage and market leadership in various ways, including obtaining

[117] For example, see Jeff Abramson, "Export Control Reform: Grading the Obama Administration's Conventional Arms Control Record," Arms Control Association, February 9, 2011, https://www.armscontrol.org/blog/2011-02-09/export-control-reform-grading-obama-administrations-conventional-arms-control-record
[118] Acton, "On the Regulation of Dual-Use Nuclear Technology," p.35.
[119] ibid, p.34
[120] ibid, p.35
[121] Scott Kennedy, "Made in China 2025," Center for Strategic and International and Studies (June 1, 2015) at: https://www.csis.org/analysis/made-china-2025.

technology from American companies and universities in priority areas, such as aerospace, AI, advanced manufacturing, new materials, robotics, and semiconductors.[122] China adopted a comprehensive AI development strategy in 2017 to "build China's first-mover advantage in the development of AI."[123] That year it also established a Central Military-Civil Fusion Development Committee to improve the Chinese military's ability to use commercial products, somewhat similar to Defense Secretary Perry's efforts in the 1990s.

During Obama's second term, officials in the Defense Department undertook what they called the Third Offset initiative, a strategy for using emerging technologies to re-establish U.S. military predominance over great power rivals despite mandatory reductions in military spending anticipated under the Budget Control Act.[124] Proponents believed that China and Russia had made significant improvements in their warfighting capabilities while the United States was bogged down in wars in Iraq and Afghanistan, particularly in their ability to deny the U.S. access to areas in their region needed for military operations. The Third Offset initiative sought greater cooperation between Silicon Valley and the Pentagon to translate U.S. advantages in AI, cyber capabilities, unmanned systems, and other emerging technologies more efficiently and better offset, or "overmatch" advances in Chinese and Russian military capabilities. It also tried to re-orient U.S. relations with those two countries, from engaging them as potential economic and diplomatic partners to treating them as strategic competitors.[125]

In 2015, DOD created the Defense Innovation Unit Experimental (DIUx) to establish partnerships with companies working on emerging technologies who were not traditional defense contractors. By this time, business R&D spending was three times greater than federal R&D expenditures, making newer tech companies more independent and more likely to make decisions based purely on market considerations than companies who considered the U.S. government to be their most important customer.[126] This is a clear contrast to industry players' attitudes during the Cold War, when they often worked to respond to the government's military-related needs. The private sector's leadership in innovation also means that the government is likely to be one step behind, making it more difficult for authorities to control products developed by private firms.

In addition, some of the leading tech entrepreneurs distrust government officials, dislike bureaucratic regulations, and have market incentives to refuse government requests for help with security matters.[127] For example, after a 2015 mass shooting in San Bernardino, California,

---

[122] "U.S. Export Controls and China," CRS In Focus (updated March 24, 2022).
[123] Graham Webster, Rogier Creemers, Paul Triolo and Elsa Kania, Full Translation: China's "New Generation Artificial Developmnt Plan," New America, August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/
[124] Reagan Defense Forum: The Third Offset Strategy, Department of Defense, November 7, 2015, https://www.defense.gov/News/Speeches/Speech/Article/628246/reagan-defense-forum-the-third-offset-strategy/
[125] Gentile et al, A History of the Third Offset, p. 3. The First and Second Offsets involved U.S. use of technological advantages, including nuclear in the 1950s and precision guidance in the 1980s to compensate for larger Soviet conventional military forces.
[126] NSF 22-320.
[127] Darren E. Tromblay and Robert G. Spelbrink, *Securing U.S. Innovation: The Challenge of Preserving a Competitive Advantage in the Creation of Knowledge* (Lanham, MD: Rowman & Littlefield, 2016)

Apple refused government requests to aid its investigation by developing new software to provide a "back door" into the shooter's iphone. A lengthy legal battle ensued, with Apple insisting that forcing companies to help the U.S. government in this way would also facilitate access by malicious actors – repressive foreign governments, intelligence agents, and cyber criminals.[128] In a reverse form of the typical dual-use dilemma, private industry exercised its power to deny U.S. officials access to a capability that they sought for legitimate reasons, for fear that somebody might eventually misuse it. As with other access-denial attempts, the seeker (in this case, the FBI) eventually found a work-around: it dropped the legal case against Apple in 2016 after an Australian security firm exploited a software vulnerability to hack into the shooter's phone.[129] The episode was indicative of the U.S. officials' need to develop a more collaborative relationship with tech industry leaders, which would be hard if they thought that strategic trade controls were preventing lucrative business deals with foreign partners.

An uneasy consensus develops against China as a high-tech peer competitor

The concerns that motivated DOD's Third Offset initiative to counter strategic advantages that China might get by surpassing the United States in key emerging technology sectors gained broader bipartisan support during the Trump and Biden administrations. When Donald Trump took office in 2017, many Democrats in Congress and large segments of the U.S. business community were very skeptical about major elements of his "America First" approach to international relations. However, they increasingly shared his perception of China as a dangerous peer competitor in a highly interdependent global economy and for leadership in technological innovation, not just in the military sphere as the Soviet Union had been. This shared perspective drove Congress to pass two major pieces of legislation expanding export controls and investment reviews to cover emerging technology and focusing more on China, without addressing whether that should be done instead of, or in addition to, the previous objective of preventing WMD proliferation. A key part of President Trump's election platform was to take a tougher approach to Chinese trade practices than his predecessors.[130] A trade war ensued with much of the economic fallout from imposed tariffs negatively affecting U.S. businesses. Several studies found that U.S. companies bore much of the cost of U.S. tariffs imposed on imports, with one estimate totaling $46 billion.[131] At the same time, the Trump administration used threats to impose tariffs and reduce military support to coerce U.S. allies into making trade concessions to the United States and increasing their military spending, moves that made Congressional Democrats and allies fear that the United States was becoming even more unilateralist and isolationist than the Bush administration had been.

---

[128] Jon Russell, "Tim Cook Says Apple Won't Create Universal IPhone BackDoor for FBI," https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/

[129] Mitchell Clark, "Here's how the FBI managed to get into the San Bernardino shooter's iPhone," *The Verge*, April 14, 2021, https://www.theverge.com/2021/4/14/22383957/fbi-san-bernadino-iphone-hack-shooting-investigation

[130] John Bolton, "The Scandal of Trump's China Policy," *WSJ*, June 17, 2020, https://www.wsj.com/articles/john-bolton-the-scandal-of-trumps-china-policy-11592419564

[131] Ryan Hass and Abraham Denmark, "More pain than gain: How the US-China trade war hurt America," *Brookings Institution*, August 7, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/08/07/more-pain-than-gain-how-the-us-china-trade-war-hurt-america/.

In late 2017, the Trump administration released a new NSS that embraced much of the thinking about emerging technologies and strategic competition with China generated by the Third Offset initiative.[132] It identified great power competition, proliferation, and transnational terrorism as three equally important security challenges, and rejected the idea that bringing China and Russia into the global trading system would promote economic and political liberalization of those autocratic regimes while providing reciprocal benefits for U.S. prosperity and security. The NSS called for a major effort to rebuild the U.S. defense industrial base and regain across-the-board U.S. military superiority to prevail in great power competition, deterrence, and potential war. It recognized the need for closer cooperation with industry and academia, both to educate them about the various ways in which strategic rivals sought to steal intellectual property and accelerate their own emerging technologies research, and to streamline the acquisition process so that the U.S. military could field transformative capabilities more quickly. Yet, some of the priority actions it proposed to take, such as tightening restrictions on foreign investment in U.S. tech companies and visas for students from countries like China to study in STEM fields at U.S. universities, were often criticized by the same industry and academic leaders whose cooperation they needed.

Soon after the new NSS came out, DIUx issued a report that made explicit why the administration intended to work with Congress to ensure that the Committee on Foreign Investment in the United States (CFIUS) was carefully evaluating national security risks. CFIUS is an interagency committee established by President Ford in the mid-1970s to review foreign investments in the United States that might be problematic, especially by wealthy Organization of Petroleum Exporting Countries. In the late 1980s, when some Americans worried that Japan might soon surpass the United States as a global economic power and technological innovator, Congress gave the president authority to block the Fujitsu Company's proposed purchase of an American semiconductor company and other proposed foreign acquisitions, takeovers and mergers if they could harm national security. The DIUx report documented a significant increase in Chinese-origin venture funding in U.S. companies over the previous seven years. It also supported claims that Chinese investments were concentrated in the same key technology areas (such as AI) that the Pentagon saw as essential for maintaining technological superiority.[133]

Concerns about Chinese IP theft, investments in U.S. companies, and advances in key militarily significant technological sectors resulted in amendments to two key pieces of legislation in 2018: the Foreign Investment Risk Review Modernization Act (FIRRMA) and the Export Control Reform Act (ECRA). FIRRMA expanded CFIUS' jurisdiction to address national security risks that might arise from non-controlling foreign investments in certain companies involved with key emerging technologies, critical infrastructure, and sensitive personal data. It did not

[132] See, Trump administration's National Security Strategy, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[133] Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," Defense Innovation Unit Experimental, January 2018. https://nationalsecurity.gmu.edu/wp-content/uploads/2020/02/DIUX-China-Tech-Transfer-Study-Selected-Readings.pdf

explicitly target any one country but was widely understood to be a direct response to the perceived threat posed by China.[134]

ECRA is the first export control legislation to explicitly treat economic security as part of national security. It underscores the importance of ensuring that trade, technology, and investment decisions do not erode the U.S. defense industrial base, make U.S. firms less competitive, or slow innovation. At the same time, it restored permanent statutory authority to the President to control dual-use technology transfers; he had been using emergency Executive powers to do so since 2001. ECRA's Section 1758 mandated that the President establish an interagency process to supplement existing controls on WMD-related technologies with new controls on "emerging and foundational" dual-use technologies, without defining those terms.[135] It said nothing, though, about how this process was supposed to weigh the potential harm to national security from overly broad export controls that slowed U.S. economic growth and technological innovation versus the security risks associated with whatever foreign rivals might gain from trade, technological collaboration, and investment involving U.S. companies and academics working on emerging technologies.

The Commerce Department's BIS initiated the Advanced Notice of Proposed Rulemaking (ANPRM) process for emerging technologies in 2018 by laying out 14 different categories for public comment:

1. Biotechnology
2. AI and machine learning
3. Position, navigation, and timing technology
4. Microprocessor technology
5. Advanced computing technology
6. Data analytics technology
7. Quantum information and sensing technology
8. Logistics technology
9. Additive manufacturing (e.g., 3D printing)
10. Robotics
11. Brain-computer interfaces
12. Hypersonics
13. Advanced materials
14. Advanced surveillance technologies

The rulemaking process caused uncertainty in the U.S. technology sector over the scope of future controls on foreign investments and sales. Some of the technologies on this list, such as hypersonics, have been under development for decades, and others, such as position, navigation, and timing technology, contributed significantly to the United States' post-Cold War RMA.

[134] For summary of FIRRMA, see "Summary of the Foreign Investment Risk Review Modernization Act of 2018," https://home.treasury.gov/system/files/206/Summary-of-FIRRMA.pdf
[135] Peter Lichtenbaum et al. "Defining 'Emerging Technologies': Industry Weighs In on Potential New Export Controls," *China Business Review*, April 17, 2019, https://www.chinabusinessreview.com/defining-emerging-technologies-industry-weighs-in-on-potential-new-export-controls/

Some U.S. companies including Amazon and Genentech took issue with defining AI and biotechnology, respectively, as "emerging" because they are well-developed technologies with global scope.[136] Other industry players questioned how the U.S. government would evaluate foreign availability and measure the impact of new controls on economic competitiveness and technological leadership.[137]

Despite disagreement about precisely what constitutes an "emerging technology," there is a general view that this term connotes "a radically novel and relatively fast growing technology characterized by a certain degree of coherence persisting over time and with the potential to exert a considerable impact on the socio-economic domains which is observed in terms of the composition of actors, institution, and patterns of interactions among those, along with associated knowledge production process."[138] Because an emerging technology's importance is based on its future capabilities and applications, there is, by definition, great uncertainty and ambiguity about its scientific promise, commercial appeal, military utility, and impact on socio-political relations. Russian interference in the U.S. 2016 presidential election and other so-called "gray zone" operations have blurred distinctions not only between war and peace, but also between military and civilian uses of technology,[139] making it even harder to get agreement on governance mechanisms than it usually is for more established dual-use technologies.

While BIS was taking public comments about potential new controls on emerging technologies, the Trump administration took other steps to restrict export of technologies and know-how. For example, it removed the civil-end user exemption for countries that are a national security concern including China, after elevating India to Strategic Trade Authorization Status 1, the same level as NATO countries.[140] Ending the civil-end user exemption for China complicated the hiring process for U.S. industry players that had previously relied on Chinese talent to develop a range of dual-use technologies including integrated circuits, and radar systems, because giving a foreign national information about a controlled technology through academic research or employment in a U.S. company is a "deemed export" that must be licensed.[141] Critics argued that export restrictions had negative implications for labor and productivity in critical technology

[136] See "Comment on Advanced Notice of Proposed Rulemaking Regarding Review of Controls for Certain Emerging Technologies," https://www.regulations.gov/document/BIS-2018-0024-0214 and Genentech, Inc.s Comments on the Advance Notice of Proposed Rulemaking Regarding Review of Controls for Certain Emerging Technologies" February 21, 2021, https://www.regulations.gov/document/BIS-2018-0024-0139

[137] "Qualcomm Comment Concerning Export Controls on Emerging Technology-PUBLIC," BIS Public Comment, February 2, 2019, https://www.regulations.gov/document/BIS-2018-0024-0183

[138] Daniele Rotolo, Diana Hicks, and Ben Martins, "What is an Emerging Technology?" *Research Policy* vol. 44, pp. 4, 2015, http://sro.sussex.ac.uk/id/eprint/56071/1/2015RP_Rotolo_Hicks_Martin_Preprint.pdf.

[139] "Deterrence Theory and Gray Zone Strategies," in *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, 2017.

[140] "Elimination of License Exception Civil End Users (CIV) – Final Rule," *Bureau of Industry and Security*, 85 FR 23470, April, 28, 2020, https://www.federalregister.gov/documents/2020/04/28/2020-07240/elimination-of-license-exception-civil-end-users-civ

[141] Evan Burke, "Trump-Era Policies Toward Chinese STEM Talent: A Need for Better Balance," *Carnegie Endowment for International Peace*, March 2021, 7, https://carnegieendowment.org/2021/03/25/trump-era-policies-toward-chinese-stem-talent-need-for-better-balance-pub-84137

industries and created an environment of uncertainty for U.S. industry, which could result in offshoring R&D.[142]

The Trump administration paid particular attention to the semiconductor industry in its broader efforts to gain strategic advantage by securing U.S. supplies and denying access to China. It placed 25% tariffs on semiconductor imports from China after an investigation into China's intellectual property theft and other unfair trade practices.[143] President Trump also added Huawei, a Chinese smartphone and telecommunications equipment firm, to the Entity List in 2019, citing espionage concerns. This policy was a clear escalation in the strategic competition between the two countries with implications for the broader semiconductor industry.[144] The entity list designation made it far more difficult for Huawei to acquire U.S. technology for its products because of U.S. export license requirements. Huawei initially adapted to the policy by purchasing semiconductors needed for its 5G network from alternative suppliers in South Korea and Taiwan.[145] In May 2020, the Commerce Department responded by amending the foreign direct product rule (FDPR) to prevent any U.S.-origin commercial off-the-shelf product from ending up in the hands of Huawei or any affiliates on the Entity List.[146] This was a direct attempt to keep alternative semiconductor technology suppliers from doing business with Huawei, since these companies often used some U.S. origin equipment in their manufacturing process.

American firms (including Applied Materials, Lam Research, and KLA) hold a large enough share of the market for semiconductor manufacturing equipment that the Trump administration could deny Huawei access to a reliable supply of advanced semiconductors, at least for a while.[147] But, achieving this security objective did predictably broad economic damage to U.S. industry players and companies in friendly countries. SEMI, an industry association representing electronics design and manufacturing, estimated that the May 2020 rule had cost $17 million in lost sales of U.S.-origin items "unrelated to Huawei" by July of that year.[148] European allies also expressed concern with the new American push for tighter export restrictions. Some European countries viewed it as a blunt instrument and were skeptical of the Trump administration's objectives, considering his broader campaign to counter China's rise.[149] By the end of Trump's time in office, Europe had yet to fully grapple with the changing realities of emerging technologies because of differences in opinion with the United States over the usefulness of export controls and the threat posed by China.[150]

---

[142] ibid., 4
[143] ibid., 2.
[144] Raymond Zong, "Trump's Latest Move Takes Straight Shot at Huawei's Business," *NYT*, May 16, 2019. https://www.nytimes.com/2019/05/16/technology/huawei-ban-president-trump.html
[145] Brown, "semiconductor industry," 26.
[146] Kay C. Georgi et al. "BIS Expands the Huawei Foreign Direct Product Rule to Capture a Wide Swath of COTS Products," *Arent Fox*, August 2020, https://www.arentfox.com/perspectives/alerts/bis-expands-the-huawei-foreign-direct-product-rule-capture-wide-swath-cots
[147] Chad P. Brown, "How the United States marched the semiconductor industry into its trade war with China," Peterson Institute for International Economics, WP 20-16, 27.
[148] See, "SEMI STATEMENT ON NEW U.S. EXPORT CONTROL REGULATIONS," https://www.semi.org/en/news-media-press/semi-press-releases/semi-export-control
[149] "Export controls and the US-China tech war," *Merics*, China Monitor, March 18, 2020, https://merics.org/en/report/export-controls-and-us-china-tech-war
[150] ibid.

Recent developments

The Biden administration has continued the Trump administration's efforts to deny China, and other countries of concern, access to high-tech information, products, materials, and manufacturing capabilities, but it has sought to take more of an *allies versus adversaries* approach than a purely unilateralist response to the perceived economic and security threat posed by the return of great power competition.[151][152] Biden officials have followed Trump's lead in the use of the entity list to block exports to specific Chinese companies in technology areas like quantum computing.[153] They have also relied on the Critical and Emerging Technology list to guide regulatory actions. In February 2022, the Biden administration added some new categories, such as Advanced Nuclear Energy Technologies, and identified subfields for each technology.[154] The executive subcommittee list significantly overlaps with and will inform future actions taken by BIS in its own efforts to control emerging and foundational technologies. The list also indicates areas where Chinese investment will be highly scrutinized by CFIUS.[155]

Most recently, the Biden administration implemented sweeping export controls on advanced semiconductors and semiconductor manufacturing equipment to China in an attempt to hobble the country's progress in advanced chip production.[156] While the Biden administration consulted with allies, the restrictions were essentially unilateral.[157] At the same time, the administration is working with U.S. allies and partners to develop a reliable and secure technological ecosystem. For example, the Quadrilateral Security Dialogue, consisting of Australia, India, Japan and the United States, is working to establish standards on AI and bolster the resilience of the semiconductor supply chain.[158]

---

[151] Alex Leary and Bob Davis, "Biden's China Policy Is Emerging—and It Looks a Lot Like Trump's," Wall Street Journal, June 10, 2021. https://www.wsj.com/articles/bidens-china-policy-is-emergingand-it-looks-a-lot-like-trumps-11623330000

[152] Antony J. Blinken, "The Administration's Approach to the People's Republic of China," U.S. Department of State, May 26, 2022. https://www.state.gov/the-administrations-approach-to-the-peoples-republic-of-china/

[153] Federal Register, Vol. 86, No. 225, Friday, November 26, 2021

[154] "CRITICAL AND EMERGING TECHNOLOGIES LIST UPDATE," Fast Track Action Subcommittee on Critical and Emerging Technologies, National Science and Technology Council, February 2022. https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

[155] Chase D. Kaniecki & Pete Young, "Cleary Foreign Investment and International Trade Watch," Clearly Gottlieb, February 17, 2022. https://www.clearytradewatch.com/2022/02/updates-to-the-critical-and-emerging-technologies-list-signal-additional-areas-of-focus/

[156] BIS, "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China," Oct. 17, 2022, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file.

[157] Gregory C. Allen, "Choking Off China's Access to the Future of AI," CSIS, October 11, 2022, https://www.csis.org/analysis/choking-chinas-access-future-ai.

[158] White House, "Fact Sheet: Quad Leaders' Summit," September 24, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/

The bipartisan consensus in Congress that more tools must be developed to counteract the PRC has grown. This includes proposed legislation that (for the first time) scrutinizes outbound U.S. foreign direct investment, as well as other business activities such as offshoring, in sectors that provide "national critical capabilities." The legislative effort also supports the identification of supply chain vulnerabilities based on reporting requirements to minimize risks in these critical areas.[159] Lack of consensus on scope of the legislation and breadth of "national critical capabilities" has produced pushback from industry and some members of Congress. Yet, fear of China getting ahead of the United States in emerging technologies with potentially transformative military applications has made an expanded role for government regulation of economic activity more palatable to many lawmakers, at least in principle, than it has been since right after World War II. Human rights concerns have further broadened Congressional support for export controls on advanced surveillance equipment and other emerging technologies that could be used by China or other repressive governments.

Despite this widespread desire among U.S. policymakers for enhanced controls on emerging technologies, regulators have made slow progress defining what should be controlled and getting multi-stakeholder agreement on which new restrictions would provide large enough security benefits to outweigh the economic, technological, and political costs. In May 2022, BIS abandoned its efforts to differentiate between emerging and foundational technologies and now refers to everything on this list as "Section 1758 Technologies."[160] This prompted a member of Congress to complain that BIS had identified "zero 'foundational' technologies, calling the terminological change a "blatant attempt" by BIS to shirk its legal responsibility and obscure oversight.[161]

As of May 2022, BIS had established 38 emerging technology controls, mostly in agreement with the Wassenaar Group or the Australia Group, whose members harmonize decisions about exports that could be used for biological or chemical weapons development.[162] In August 2022, BIS added only four more very narrowly defined emerging technologies to the CCL: two substrates of ultra-wide bandgap semiconductors, electronic computer-aided design software for the development of integrated circuits for a particular type of transistor structure (GAAFET), and pressure gain combustion technology used in gas turbine engines. The BIS interim final rule noted that these four technologies met "Section 1758 Technologies" criteria and had been added to the Wassenaar Arrangement control list the previous December.[163] BIS promised to address

[159] Sarah Bauerle Danzman, "Is the US going to screen outbound investment?," Atlantic Council, January 10, 2022. https://www.atlanticcouncil.org/blogs/econographics/is-the-us-going-to-screen-outbound-investment/
[160] Federal Register, Vol. 87, No. 99, Monday, May 23, 2022 (Proposed Rules)
[161] "McCaul on BIS Decision to Change Terminology, Dodge Statutory Responsibility," House Foreign Affairs Committee, May 25, 2022. https://gop-foreignaffairs.house.gov/press-release/mccaul-on-bis-decision-to-change-terminology-dodge-statutory-responsibility/
[162] Tongele N. Tongele, "Emerging and Foundational Technology Controls," presentation to the Association of University Export Control Officers, May 4, 2022, https://researchservices.upenn.edu/wp-content/uploads/2022/04/Emerging-and-Foundational-tech.pdf.
[163] BIS "Implementation of Certain 2021 Wassenaar Arrangement Decisions on Four Section 1758 Technologies," 87 FR 49979, August 15, 2022. https://www.federalregister.gov/documents/2022/08/15/2022-17125/implementation-of-certain-2021-wassenaar-arrangement-decisions-on-four-section-1758-technologies

decisions taken at the same WA plenary meeting to loosen controls on other technologies at a future time.[164]

Although the Biden administration has been more concerned than its predecessor about cooperating with allies to enhance the effectiveness of export controls, it has taken several unilateral steps to try to maximize the United States' relative advantage over China in what it considers the three most critical emerging technology sectors: advanced computing (including microelectronics, quantum information systems, and AI), biotechnology, and clean energy.[165] In August 2022, it gained bipartisan support for the CHIPS and Science Act, which provides over $52 billion of public funding, and leverages a comparable amount of private sector money, to re-establish U.S. leadership in advanced semiconductor research and manufacturing.[166] Two months later, the administration announced new export restrictions on advanced computer chips and chip making equipment that China could use to modernize its conventional and nuclear capabilities. Since all the most advanced semiconductors are currently made in Taiwan and the most sophisticated lithography equipment needed to make these chips is only manufactured by one company in the Netherlands, the United States invoked the FDPR to try to prevent these and other foreign companies using any American technology from exporting banned items to China.

Several features of the advanced semiconductor sector help explain why the Biden administration focused narrowly on this subset of advanced computing for its first major new application of U.S. export controls. The most advanced U.S. supercomputing capabilities have been subject to export reviews and restrictions since the Cold War, so this has long been considered a dual-use technology with particularly significant security implications. A foundation of bipartisan political support had already been laid during the Trump administration for the idea that denying China access to advanced chips was a chokepoint that would provide broad strategic economic, military, and technological advantages for the West at relatively low cost. There are also good reasons why the U.S. semiconductor industry would be enthusiastic about this initiative. It gained a huge infusion of government funding to help it achieve and potentially surpass what a few companies in Asia and Europe are already able to do, plus the imposition of FDPR controls on those foreign companies' ability to sell to China, in return for not exporting some of their best products to China.[167]

Even under these relatively conducive circumstances, it is hard to know how much of a strategic advantage these new U.S. export controls will provide and how long it will last. U.S. officials

---

[164] "Wassenaar Posts Export Control Changes From 2021 Plenary," *Export Compliance Daily*, December 27, 2021, https://exportcompliancedaily.com/news/2021/12/27/Wassenaar-Posts-Export-Control-Changes-From-2021-Plenary-2112230061.

[165] "Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit," September 16, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/.

[166] See, CHIPS and Science Act FACT SHEET, 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/.

[167] Martijn Rassner and Kevin Wolf, "The Right Time For Chip Export Controls," Lawfare Blog, December 13, 2022, https://www.lawfareblog.com/right-time-chip-export-controls.

acknowledged that unilateral controls will "lose effectiveness over time if other countries don't join us, and we risk harming U.S. technology leadership if foreign competitors are not subject to similar controls."[168] Some aspects of the reasoning behind these restrictions are similar to the "naive view of the nature of technology transfer" that motivated U.S. efforts to use export controls to keep the Soviets from improving the accuracy of their missile guidance systems during the Cold War, and to keep regional powers from acquiring ballistic missiles capable of carrying nuclear warheads in the 1990s. The Chinese government is already making a concerted effort to overcome various technological weaknesses that hinder its indigenous ability to produce semiconductor manufacturing equipment capable of meeting its own needs and competing in the global marketplace, much as Japan caught up with and surpassed U.S. semiconductor manufacturing in the 1970s and 1980s.[169] As Mistry's research on the MTCR shows, the imposition of new export controls usually spurs increased indigenous investment and technological advancement, so they may delay, but rarely stop the target country from acquiring a particular capability. They might be worthwhile if the countries employing *unilateral, allies versus adversaries,* or *suppliers against seekers* strategies use however much extra time they gain from these denial-based approaches to include the target state(s) in the development of a more cooperative governance arrangement for the dual-use technology in question,[170] but there is little evidence that anyone in the Biden administration is thinking about how to engage China constructively to develop mutually acceptable rules for responsible uses of advanced computing technologies.

The unilateral imposition of strict new export controls is less feasible and desirable for other emerging technology sectors. Biotechnology and clean energy technology, the two other broad fields that the Biden administration has identified as worthy of a large investment of U.S. government funds to offset restrictions on foreign investment and exports, do not have a lengthy history of exports controls like advanced computing does. The U.S. biotech industry successfully resisted international efforts in the 1990s to negotiate a verification protocol for the Biological Weapons Convention, which would have been a *cooperative management* strategy to reduce concerns about the global spread of advanced biotechnologies. It also helped convince the Bush administration to keep the national review process for research with dangerous pathogens from being strengthened after the 2001 anthrax attacks as much as some experts recommended.[171]

Attempts to impose strategic trade controls on clean energy technologies would face strong political opposition from environmentalists around the world, as well as from many private sector interests. They are not on the "Section 1758" list, indicating that BIS is not currently considering imposing any export or investment controls in this field. The United States imposed anti-dumping tariffs on solar panels from China in 2012, but recently suspended anti-dumping

[168] Senior administration official quoted in Ellen Nakashima, Jeanne Whelen, and Cate Cadell, "U.S. Targets China's Access to High-Tech Computer Chips," *The Washington Post* (October 8, 2022).
[169] Will Hunt, Saif M. Khan, and Dahlia Peterson, "China's Progress in Semiconductor Manufacturing Equipment: Accelerants and Policy Implications," Georgetown Center for Security and Emerging Technology Policy Brief (March 2021).
[170] Dinshaw Mistry, "Beyond the MTCR: Building a Comprehensive Regime to Contain Ballistic Missile Proliferation," *International Security* 27:4 (Spring 2003) 119-149.
[171] Elisa Harris, John Steinbruner, Nancy Gallagher, and Stacy Okutani, *Controlling Dangerous Pathogens* CISSM monograph (March 2007), https://drum.lib.umd.edu/handle/1903/15592.

duties that could be levied on imported solar modules and cells from Cambodia, Malaysia, Thailand, and Vietnam in order to accelerate solar projects in the U.S., which had been stalled by the prospect of high tariffs on solar products suspected of having Chinese components.[172] A recent study projected large future cost savings from global trade in clean energy technologies by estimating that having a globalized photovoltaic (PV) module market had saved PV installers US$24 (19–31) billion in the United States, US$7 (5–9) billion in Germany and US$36 (26–45) billion in China from 2008 to 2020.[173] Staunch neo-mercantilists might argue that this could harm U.S. national security because the financial benefits are larger for China than for the United States and Germany, but most people are likely to focus on the fact that all three countries get substantial savings. The prospects for avoiding catastrophic climate change hinge on how rapidly countries and companies around the world, and especially in large, rapidly growing countries like China, can innovate, commercialize, and adopt clean energy technologies. For both economic and environmental reasons, therefore, it is hard to imagine the United States and its Western allies agreeing to impose strategic trade controls on clean energy technologies that might help China reduce its carbon emissions.

Crafting a path forward: socio-technical dimensions to guide policy decisions

Focusing just on the three categories of emerging technology that the Biden administration identified as crucial for United States and other democratic countries to "win the competition for the twenty-first century"[174] indicates how challenging it will be to get multi-stakeholder agreement that the benefits of implementing specific new strategic trade controls outweigh the economic, technological, political – and also medical and environmental costs. Each broad field differs from the others in ways that affect the feasibility and desirability of different policy options for managing its development, spread, and use to promote beneficial applications and prevent dangerous ones. The same could be said of the other twelve categories on the BIS list of emerging technologies under consideration for new strategic trade controls.

To complicate matters further, the Biden-Harris NSS takes a less purely zero-sum view of great power relations than the Trump administration did. The 2022 NSS declares that the United States, Russia, and China should "compete responsibly where their interests diverge and cooperate where they converge," highlighting climate and energy security, biosecurity and pandemics, food security, arms control and nonproliferation, and terrorism as shared challenges where mutually beneficial cooperation should be possible.[175] This raises fundamental questions about whether and when the primary objective of emerging technology governance policies should be:

- Advancing U.S. national interests unilaterally (America first);

[172] https://www.jdsupra.com/legalnews/president-biden-announces-2-year-1095176/.
[173] https://www.nature.com/articles/s41586-022-05316-6.
[174] Biden-Harris Administration National Security Strategy, October 2022, p. 3, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf
[175] Biden-Harris NSS, pp. 27-31.

- Maximizing the United States and its democratic allies' relative power vis-a-vis authoritarian governments;
- Establishing "guardrails" for great power competition to enhance strategic stability and avoid excessive arms racing;
- Coordinating suppliers' decision-making about selling dual-use technologies to potential proliferators and terrorists seeking WMD; or
- Institutionalizing norms, regimes, and other cooperative management arrangements to promote beneficial uses of emerging technologies, increase transparency, provide reassurance, and respond collectively to hostile or irresponsible actions by state and nonstate actors.

In current policy debates, the main motivation for tighter controls has shifted from concerns about WMD proliferation to strategic competition with a great power rival whose economic power and technological advancement are closer to the United States' than those of the Soviet Union ever were, without much debate about which is actually the more urgent security problem. Nor has there been much open discussion about how well denial-based control mechanisms are likely to work when the global economy remains highly integrated, and when companies need to maximize profits and governments need to foster economic growth under difficult conditions. In this context, policymakers must avoid two types of errors, both of which have been made repeatedly before. They do not want to be paralyzed by complexity to the extent that unregulated dual-use technologies can be easily obtained or developed and used to harm vital U.S. interests. But they also should be careful not to impose strategic trade controls on broad areas of emerging technology if they are not likely to be effective, and if the economic, political, and technological development costs are likely to outweigh any security benefits that can be achieved.

The historical analysis of previous U.S. efforts to manage dual-use technologies during and after the Cold War showed that what governance approaches were chosen, and how well they worked, was a function of the international security and economic context; the characteristics of the technology in question; the state of that technology's development and diffusion; and the relevant stakeholders' interests and ideas about managing dual-use technology. Therefore, policymakers should approach governance of emerging dual-use technologies by considering both the general factors structuring the current iteration of this policy dilemma, and the specific socio-technical characteristics of each type of emerging technology that raises dual-use concerns.

The global security and economic context is roughly the same for all current categories of emerging dual-use technology, but each type contributes in different ways to national security and economic growth, depending on specific features of that sector. Important technological characteristics to consider include expectations and uncertainty about scientific promise; whether technologies are primarily made up of material or intangible components; and how demanding the fabrication process is. Some dual-use emerging technologies may be developed primarily in the private sector and used for commercial and civilian purposes, with relatively few current military applications, while others may be predominantly developed with government funding for military applications. Some so-called "emerging" technologies are still at such an early stage

of development that imposing controls would stifle innovation without any near-term security benefits, while others have already been commercialized by so many companies in different countries that imposing effective controls is simply not possible, regardless of what the rationale might be. Finally, some or all of the major powers may be competing for advantage on the frontier of technology development, with important implications for strategic stability, whereas other emerging technologies are primarily of concern as they affect WMD proliferation.

To illustrate how these types of technology-specific considerations impact the feasibility and desirability of various governance options, this remainder of this section will summarize findings from earlier CISSM research that mapped sectoral characteristics for five types of emerging technologies drawn from categories on the BIS's 2018 ANPRM list.[176] It examined positioning, navigation, and timing (PNT) technologies, quantum computing, quantum sensing (two different sectors lumped together on the BIS list under quantum information and sensing), hypersonics, and computer vision (a distinct subset of the much larger BIS category of AI and machine learning).

These five technologies were selected for analysis based on a review of the stakeholder commentary provided in response to the ANPRM, to account for different stages of development, degrees of dual-use application, and technological factors. Data was collected for each technology across a range of variables that have been identified in the academic literature and policy debates as potentially relevant to the desirability and/or feasibility of denial-based control options (unilateral, allies versus adversaries, and suppliers against seekers) because those are the options most commonly discussed at this time.

Seven technology-specific characteristics emerged from this sectoral mapping exercise as particularly important. Some primarily affect feasibility – i.e. how realistic it is that some type of denial-based control strategy could prevent or slow countries of concern acquisition of the capability in question. Others primarily influence desirability from the perspective of various stakeholders – i.e., how they view the military, economic, political, and technological benefits or costs of different types of governance options.

The emerging technology sectoral mapping study was conducted independently of, and largely prior to, the historical analysis of the nature and effectiveness of U.S. strategies for managing dual-use technologies presented earlier in this paper. The technological and sociological factors that shaped choices about what type and scope of controls should be applied to a specific technology in a particular security and economic context, and that determined how effectively those policies provided the desired security benefits without excessive economic, political, and technological costs, are clearly relevant to current efforts to manage emerging technologies. For

[176] Lindsay Rand, Tucker Boyce, and Andrea Viski, *Emerging Technologies and Trade Controls: A Sectoral Composition Approach*, Strategic Trade Research Institute and Center for International & Security Studies, U. Maryland, 2020. *JSTOR*, http://www.jstor.org/stable/resrep26934.1. Hereafter CISSM 2020 Report.
Lindsay Rand, "Quantum Sensing Sectoral Analysis," Center for International and Security Studies, U. Maryland, Working Paper, 2021.
Lindsay Rand, Dimitri Nilov, C.J. Horton, "Hypersonic Technology Sectoral Analysis," Center for International and Security Studies, U. Maryland, Working Paper, 2021.

example, unlike technologies in the historical analysis, an important contemporary consideration is the extent to which the technology innovation of interest is captured by software components. As more innovation occurs on software, rather than hardware, for emerging technologies, the applicability of historical controls which are based on tracking tangible items shrinks. The traits considered in the emerging technology sectoral mapping attempt to capture these new trends by considering the technological and sociological shifts that will influence the applicability of different types of controls.

The following subsections summarize those characteristics, then provide a top-level comparison of those characteristics in the five emerging technology sectors used as case studies in the earlier mapping studies. This shows that while there might be broad bipartisan consensus in principle on the desirability of enhanced strategic trade controls on emerging technologies, it will be difficult to identify many feasible options. It also indicates that as policy debates move from evaluating the general desirability of strategic trade controls on emerging technologies to consideration of the specific options that might be feasible, it will probably be even more difficult to get multi-stakeholder agreement in practice on which measures are likely to provide security benefits that outweigh the technological, economic, and political costs of trying to impose tighter controls.

Technology-specific feasibility considerations

Characteristics such as technology makeup, the fabrication process, and the stage of development during the period of consideration are influential in determining how feasible it might be for the U.S. government to impose tighter unilateral trade controls on a broad area or specific application of an emerging technology, whether it could achieve its security objectives by cooperating on controls with allied countries and/or with other supplier states, or whether the only available options involve consensual agreement on rules for responsible use.

1. Technology Makeup

The feasibility of various control or regulatory policies depends in part on what types of systems and components comprise the technology. For hardware-based systems or systems that have critical hardware components, there may be limited sources of critical raw materials or intricate components. In these cases, it could be feasible to control the flow of the technology through limiting access to a critical node in the supply chain. Whether the United States is the sole producer of the protected node, or the degree to which the countries that have access are among a cohort of allies or a group with a shared interest in control, will determine the feasibility of establishing effective unilateral or multilateral controls.[177] However, exclusion-based controls also could lead to the unintended consequence of incentivizing indigenous capability acquisition or development of alternative methods to achieving the technology in the very country or countries for which the controls were intended to target, and thus may actually facilitate broader dispersion in the long run. As discussed previously, an unintended consequence of the Clinton

[177] For example, also discussed as Category II items in: "UAV Export Controls and Regulatory Challenges," Stimson Working Group Report, 2015, https://www.stimson.org/wp-content/files/file-attachments/ECRC%20Working%20Group%20Report.pdf.

Administration's MTCR strategy was that it catalyzed India's now robust aerospace technology industry.[178]

Conversely, if a technology is almost entirely software-based, control mechanisms cannot target the physical movement or ownership of hardware components. Instead, governance of intangible technology transfers must address software applications, sometimes referred to as "end-use controls". These types of controls are more challenging because intent, and even application, are more difficult to verify than physical technology development and possession.[179] This challenge is becoming a larger problem for the export control community, as the key innovation elements of new technologies gradually become more software-based. An added challenge is the fact that cloud-based systems establish vast networks of dispersion, allowing remote access to physical systems and data, and sometimes without a user's knowledge that such dispersion may occur.[180] The increased role of software among current emerging technologies is one of the core challenges to the traditional export control paradigm.

2. Technology Fabrication Process

The fabrication process for military and dual-use technologies has historically been a very active area of consideration in proliferation analysis.[181] This dimension includes the design, manufacturing, and testing phases required for developing a given technology. It also encompasses the facilities needed, and the tacit knowledge or human resources required to ultimately develop and operate the technology. Controls on critical fabrication processes and requirements can further increase the timeline for potential proliferators to achieve a technology, but the efficacy of such a policy varies depending on the sophistication of the fabrication process and requirements. If these processes and requirements are very expensive or difficult to acquire, barriers to entry are higher, and the number of countries and companies making and transferring the technology will be smaller even without the implementation of control mechanisms than would be true for a technology that is equally valuable and easier to fabricate.

Conversely, in cases where technologies have extremely high fabrication requirements, countries may pursue cooperative agreements to pool resources and increase economic efficiency to lower this barrier. The United States and United Kingdom collaborated for this reason when developing the first atomic bomb during World War II, as did the Reagan administration when it initiated military co-development agreements to share costs and expertise with allies.[182] Similar strategies

[178] For example, U.S. controls limiting Indian access to critical space technologies incentivized a long-term effort to develop a robust Indian space technology sector.
[179] Mark Bromley and Giovanna Maletta, "The Challenges of Software and Technology Transfers to Non-Proliferation Efforts: Implementing and Complying with Arms Control," SIPRI, April, 2018, https://www.sipri.org/publications/2018/other-publications/challenge-software-and-technology-transfers-non-proliferation-efforts-implementing-and-complying.
[180] "Cloud Computing: The Concept, Impacts and the Role of Government Policy," OECD - Digital Economy Papers, No. 240, https://www.oecd-ilibrary.org/science-and-technology/cloud-computing-the-concept-impacts-and-the-role-of-government-policy_5jxzf4lcc7f5-en.
[181] For example, discussed in: Donald MacKenzie and Graham Spinardi, "Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons," *American Journal of Sociology*, Vol. 101, No. 1, July 1995.
[182] Margaret Gowing, *Britain and Atomic Energy* (New York: St. Martin's Press, 1964).

are being tried in the current environment of great power technology competition, as evidenced by a new set of cooperative agreements over quantum information science with the United Kingdom, France, Australia, Japan, Denmark, Sweden, Finland, and Switzerland.[183] Cooperating on technology development has potential downsides. It often stokes fear of technology proliferation via the entities in the collaborating country and beyond U.S. control, a process called "leakage."[184] It can also raise concerns about firms in countries that collaborate with the United States on technology development soon outcompeting U.S. companies in global high-tech markets – a key finding of OTA's 1990 *Arming our Allies* report that resonates with some today.

Digital technologies, and technologies leveraging digital/computational tools, rely heavily on human knowledge and skill in the fabrication process. This makes the availability of an appropriately skilled workforce an important constraint on who can master a given technology and how quickly they can advance R&D to deployment and commercialization. In 2017, a National Academies report highlighted that preparing a national technical workforce capable of meeting innovation needs is a key requirement for maintaining economic and national security,[185] and the National Science Board surveyed potential solutions to prevent projected technical workforce shortages.[186]

When technologies have high requirements on specific training, skill sets, and tacit knowledge for production, human talent may become a target for control. Since many of the leading innovative research universities in the world have historically been located in the United States, some policymakers see restricting foreign students' access to higher education as a way to maintain competitive advantage, while others believe that this would hurt U.S. higher education, technological innovation, and political relations for little, if any, security gain. Further, this imposes the added costs of blocking dialogue and wider dispersion of norms and standards for emerging technology development and use, as well as limiting the potential for the United States to shape these standards. The more specialized education and training scientists, engineers, and technicians need to work with a particular technology, the more relevant codes of conduct and other professional norms for appropriate use of emerging technologies could be in facilitating cooperation on appropriate use and risk mitigation.[187]

3. Stage of Development and Dispersion

Finally, the stage of development and dispersion for a specific technology affects the types of control mechanisms that would be feasible and the consequences of different policy options. If the technology is at an early stage of development and has not yet been widely dispersed, then

[183]" US and France Sign Statement of Cooperation for Quantum Technology, November 2022, https://quantumcomputingreport.com/u-s-and-france-sign-statement-of-cooperation-for-quantum-technology/.
[184] Dov Zakheim, "Military technology cooperation with key allies outweighs the risk of leaks to enemies," *The Hill*, December 16, 2022, https://thehill.com/opinion/national-security/3776929-military-technology-cooperation-with-key-allies-outweighs-the-risk-of-leaks-to-enemies/.
[185] "Building America's Skilled Technical Workforce," *The National Academies of Science and Engineering*, 2017, https://www.nap.edu/catalog/23472/building-americas-skilled-technical-workforce.
[186] "The Skilled Technical Workforce: Crafting America's Science & Engineering Enterprise," National Science Board – Document 2019-23.
[187] For example, discussed in: MacKenzie and Spinardi, 1995.

the policy response is likely to play a formative role that may have downstream effects on the eventual technology developed. If the technology is at a fairly advanced stage of development and is already somewhat commercialized and dispersed, then the policy approach will have to be more responsive and export controls are less likely to be successful.[188]

Dispersion affects both the feasibility of different governance approaches and the relevant stakeholders whose participation would be needed for a particular denial-based control method to achieve its security objectives. The feasibility of *unilateral* approaches diminishes rapidly when the United States (or any other country trying this approach) does not have a monopoly on an entire technology or the most advanced forms of it, and on the knowledge, materials, and other components needed to master it indigenously. An *allies versus adversaries* approach can only be effective when the United States, allies, and other friendly countries have a significant lead in a particular technology and its military applications, and agree that the security benefits of maintaining or widening that lead vis-a-vis potential adversaries outweighs the various costs of implementing strategic trade controls. When the United States and one or more strategic competitors are able to produce and willing to export dual-use capabilities that are developed enough to be of proliferation concern, then the effectiveness of *Suppliers against Seekers* arrangements depends on the strategic competitors' participation (as a full member or by aligning their export control practices while remaining outside that regime, as China did with the MTCR) – even if the products they might sell a proliferator are not at the very cutting edge of that technology.

Policymakers must be aware of and realistic about the stage of development and dispersion for each technology considered so that they can identify the main corresponding risks associated with different types of policy responses. The risk of responding at earlier stages of development is that the government may push innovation away or stymie the natural innovation process and effectively limit its own eventual use of and leadership over the technology.[189] The risk of responding at later stages of development is that the government may face more obstacles backtracking dispersion/proliferation or imposing standards on a technology sector once the technology is well developed and dispersed, with robust spheres of fabrication and clientele stakeholders. Importantly, this also imposes a temporal dimension on the control evaluation framework, which means continual observation and consideration should be instituted for truly emerging technologies that may be at too early of stages for controls now, but that could evolve to more advanced stages and threaten security risks later.

Technology-specific desirability considerations

When stakeholders are assessing the desirability of different policy options to govern dual-use technologies, their preferences will be shaped both by their general orientation towards

[188] ITI Comment in Response to U.S. Department of Commerce ANPRM: https://www.itic.org/public-policy/ITICommentsECRAEmergingTechnologyANPRM.pdf.
[189] Martijn Rassner, "Rethinking Export Controls: Unintended Consequences and the New Technology Landscape, December 8, 2020, https://www.cnas.org/publications/reports/rethinking-export-controls-unintended-consequences-and-the-new-technological-landscape.

technology controls and by technology-specific factors. Political culture and ideology, for example, inform general beliefs about how much control public sector officials should have over private sector operations, while a specific stakeholder's role influences the relative importance placed on security, economic, technology innovation and foreign policy considerations when weighing pros and cons of control options. Technology-specific factors that contribute to this complex desirability matrix include the scope of dual-use applications for the technology, the magnitude of disruption posed by the technology, the mix of stakeholders participating in the technology's development, and the sheer scientific promise (sometimes related to "hype") of the technology.

1. Dual-Use Applications

The extent to which a specific technology has dual-use applications has a profound effect on the desirability of controls. If the technology has a wide array of civilian applications, for example, policymakers cannot effectively control the technology alone without incentivizing non-compliance. Instead, they will need to work with the private sector to establish actionable policies that do not negatively affect civilian applications. Conversely, if the technology is more narrowly applicable to military applications, then the government may institute stricter controls without facing criticism. Economies of scale is an important desirability consideration for dual-use technologies, because sustaining dual-use market access enables higher economic efficiency for technology developments, while technologies that are heavily restricted to military applications could require significant support from the government, especially in the absence of cooperation agreements.

For a dual-use technology with extensive civilian applications, policies must also account for other dimensions of the technology's role on national security, including economic competitiveness and domestic economic well-being. On one hand, controls intended to preserve military advantage may inadvertently damage the defense industrial base and require greater government resources. But the government may also face domestic opposition and deteriorating trust on the part of the private sector if policies are overly burdensome, which could stunt American innovation or incentivize scientists and engineers to relocate abroad. This could limit American access to economic growth or fundamentally important technology innovations, a trend that was highlighted in the historical analysis during periods of stricter controls, such as the Bush and Trump eras.

2. Disruption Mechanism

The technology-specific factor most voluminously discussed in existing literature on emerging technologies is the mechanism of disruption to established practices, norms, and relationships. Debates about controls on dual-use technologies may focus on potential disruption to established security arrangements among global powers, stronger and weaker states (e.g. "haves" and "have nots"), or state and nonstate actors. Depending on one's perspective, disruption can be dangerous or beneficial. For example, if nuclear deterrence is currently "stable" (e.g. the probability of nuclear attack during peacetime, a crisis, or a conventional conflict is low) because all countries with nuclear weapons know that they would likely face a devastating retaliatory strike, then

emerging technologies could be "destabilizing" if they increased the possibility of a disarming first strike. Some stakeholders might seek such developments as a way to gain strategic advantage, while others would see them as a dangerous form of disruption that warrants arms control. Alternatively, if uncertainty, misperceptions, and worst-case scenario planning increase crisis instability and fuel arms races, then emerging technology applications that increase transparency could be stabilizing, and thus should be encouraged rather than controlled. The spread of dual-use technologies from a small number of advanced states to a larger number of developing countries can also be disruptive in desirable or undesirable ways, depending not only on how that changes the status quo, but also on whether the change is viewed from the perspective of a stakeholder that benefited from established arrangements or one who expects to benefit from change.

Disruption, by nature of the definition of emerging technologies, is often the impetus for evaluating controls. While there will almost always be disagreement over whether the disruption is positive or negative, due to political or institutional biases, the scope of actors that reach consensus on the negative disruption potential for technology dispersion will dictate whether a control agreement will be unilateral or multilateral and take the form of an *allies versus adversaries* or a *suppliers against seekers* approach.

3. Stakeholder Community and Power Distribution of Stakeholders

The stakeholders are the primary actors that must work together to establish and implement control policies for a given technology. Each U.S. administration must work with Congress on some aspects of technology governance, and different Executive Branch agencies can have distinct preferences that must be managed through an interagency process. Depending on the stage of technology development and the form of financing, commercial firms and academic institutions can be important independent stakeholders, or they can be relatively minor, subordinate players. Finally, stakeholders can also include foreign governments, corporations, and scientists that have some claim or significance in developing the technology.

The composition and relationships of stakeholders for a given technology will determine how much and what type of cooperation is required for effective governance. During the relatively short periods when the United States was the only country that had developed military applications for a given technology (e.g., nuclear weapons and most advanced conventional weapons in the aftermath of World War II), unilateral efforts to prolong those monopolies seemed feasible and desirable to some Americans. In both cases, though, technological diffusion rapidly increased the number of stakeholders inside and outside of various control arrangements, each of whose capabilities and interests affected how well a given governance arrangement worked.

Broad consensus among diverse stakeholders is inevitably difficult. Policy options that seem desirable to some stakeholders may be unattractive or unacceptable to other stakeholders. If one stakeholder has much more legal power, economic leverage, and institutional capacity than others, they may be able to impose their preferred outcome over the weaker stakeholders' objections, at least formally. Unless the governance mechanism includes legally binding rules,

appropriate means of verifying compliance with those rules, and effective compliance management or enforcement mechanisms, though, the less desirable control mechanisms seem to various stakeholder groups, and the less likely they are to implement them fully.

4. Scientific Promise

The scientific promise for a particular emerging technology has two aspects. The current state of scientific knowledge limits how much near-term advancement is realistic. It also informs assessments of the theoretical limits on what the most advanced version of the technology could accomplish. Those theoretical limits may be understood, or there may be significant uncertainty and debate about what is technologically possible given enough time, money, and ingenuity. Appreciating both the possibilities and the limits of technological development over time, can help to temper hype and craft realistic projections about the likely security and economic impacts of new and rapidly advancing technologies. In turn, this could provide insight into whether or not controls are a needed to protect national security, or whether unrealistic projections about the "game-changing" results if hostile states or nonstate actors acquire given technology are exaggerating the desirability of tighter controls.

Technology case studies

To illustrate how differences across these seven dimensions affect the feasibility and desirability of different governance options, we analyzed the technical characteristics and industry composition for five emerging technology groups: PNT, quantum computing, computer vision, hypersonics, and quantum sensing. Computer vision and quantum computing are directly related to the advanced computing technology priority area, while hypersonics, PNT, and quantum sensing improve precision targeting capabilities in ways that have important implications both for strategic stability and nonproliferation. Some of the technologies selected for analysis, like computer vision, have broad civilian applications; others, like hypersonics are primarily suited for military purposes. Additionally, software-based technologies, such as computer vision, are not feasible to manage through existing control regimes based on hardware component management more relevant to technologies like quantum computing.

There was also heterogeneity across the technologies with respect to the extent that stakeholders and policymakers expressed desirability for controls (based on the ANPRM commentary). Hypersonics, which are primarily military, strategically destabilizing, and proliferation-prone, are attractive, if difficult, targets for controls. On the other hand, computer vision has numerous commercial applications, a tangential relation to military operations, and a clearer connection to domestic surveillance by repressive governments. In this case, there is much greater stakeholder disagreement about what, if any, controls would be desirable.

A systematic sectoral mapping exercise was conducted for each of the five technologies as part of a larger project. The resulting technology reports can be referenced for greater detail on data collection and analysis methodology, and for a more comprehensive presentation of data and

conclusions.[190] The key trends identified for each technology are summarized below, with a focus on higher level findings relevant for policies and controls based on the key feasibility and desirability dimensions for analysis identified above. The historical analysis above will also be used to assess precedent for controls based on the technology characteristics, although where necessary geopolitical trends and technological factors that distinguish the current context from historical case studies will also be identified to assess the scope of the policy challenges.

1. Positioning, Navigation, and Timing (PNT)

PNT technologies pose challenges to both the feasibility and desirability of controls. PNT technologies include technologies that help to accurately and precisely determine location, navigate to a desired position, and acquire and keep accurate timing.[191] Nominally, the importance of military PNT technology stems from its inclusion of Global Positioning System (GPS) architectures.[192] But PNT may also include technologies needed for communication and detection.[193] Within the past ten years, PNT technologies have attracted increased attention as other technology areas, such as quantum technologies, offer opportunities for improvements to PNT. Conversely, other developments such as cyber warfare have raised questions over potential vulnerabilities of existing PNT systems to spoofing or jamming. The Trump administration issued an Executive Order to strengthen resilience of PNT services,[194] which resulted in a NIST report outlining appropriate cybersecurity techniques.[195]

The PNT sector constitutes a case study of continual technology development over a long time period. In their most rudimentary form, PNT technologies have been around for centuries, and were well established by World War II. Navigation platforms that use GPS and similar systems are globally ubiquitous. Use of emerging scientific techniques to develop a new wave of advanced PNT technologies has been motivated by the need for systems that operate in signal-free environments (e.g. use dead reckoning when GPS signals have been jammed or are otherwise unavailable) and harsher domains (in space or underwater, for example) and that

[190] Lindsay Rand, Tucker Boyce, and Andrea Viski, *Emerging Technologies and Trade Controls: A Sectoral Composition Approach*, Strategic Trade Research Institute and Center for International & Security Studies, U. Maryland, 2020. *JSTOR*, http://www.jstor.org/stable/resrep26934.1. Hereafter CISSM 2020 report.
Lindsay Rand, "Quantum Sensing Sectoral Analysis," Center for International and Security Studies, U. Maryland, Working Paper, 2021.
Lindsay Rand, Dimitri Nilov, C.J. Horton, "Hypersonic Technology Sectoral Analysis," Center for International and Security Studies, U. Maryland, Working Paper, 2021.
[191] "What is Positioning, Navigation, and Timing (PNT)?" United States Department of Transportation, https://www.transportation.gov/pnt/what-positioning-navigation-and-timing.pnt.
[192] "Defense Navigation Capabilities," United States Government Accountability Office – Technology Assessment GAO-21-320SP, May 2021, https://www.gao.gov/assets/gao-21-320sp.pdf.
[193] ibid.
[194] "Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services," Executive Order 12905, February 12, 2020, https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing.
[195] Michael Bartock, Suzanne Lightman, Ya-Shian Li Baboud, James McCarthy, Karen Reczek, Joseph Brule, Doug Northrip, Arthur Scholz, and Theresa Suloway, "Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing Services," National Institute of Standards and Technology – NISTIR 8323, February 2021, https://csrc.nist.gov/publications/detail/nistir/8323/final.

optimize size, weight, power, and cost (SWaP-C) parameters.[196] Cutting-edge platforms using emerging technologies to meet these requirements, including chip-scale atomic clocks and quantum sensors, are under development, with a few extremely expensive applications already commercially available.[197]

Because advanced PNT technologies have been under development and in use for decades, it would only be feasible to impose new controls on a subset of applications that are still in an early stage of development. The technological basis for the field is fairly well dispersed across a handful of research areas.[198] The technology makeup and fabrication process for older PNT technologies is almost entirely hardware based and is relatively simple. Many PNT products are commercially available globally and it would be very challenging, if not impossible, to retroactively control or constrain access to these capabilities. Many companies, universities, and government-affiliated organizations working on emergent PNT are located in the United States, China, and Europe, with substantial collaboration among various entities in this field. This means that *unilateral* or *allies versus adversaries* types of control are much less likely to be effective than enlisting China in some type of *suppliers against seekers* arrangement. About half of the organizations surveyed for the PNT sectoral mapping analysis indicated military ties. More nascent PNT technologies do have some critical material and fabrication nodes, such as cold atom technologies, that could feasibly be restricted. The number of scientists/personnel familiar with techniques and methods at the bleeding edge of development is also currently limited. Thus, so long as there is some fundamental improvement in scientific application at a defined stage of development, feasible controls could be identified at that specific stage, although because of the historic momentum of technology, the window for implementation will likely be fairly narrow.

It is also hard to predict whether or not the narrowly defined controls on advanced PNT technologies that might be feasible would also be desirable for relevant stakeholders. U.S. policymakers who are focused on the military applications may favor imposing unilateral access controls in hopes of maintaining a strategic asymmetric technology advantage. As we have seen, similar controls were implemented during the Cold War to deny Soviet access to precision guidance technologies that the United States used for missile navigation. The Soviets, however, preferred other types of solutions to missile guidance challenges and already had sufficient, if not superior, indigenous guidance capabilities, so the security value of these controls was less than commonly believed.[199] There are also powerful commercial and civilian PNT stakeholders in the automobile and aerospace industries who will be equally interested in, and to some degree reliant on, improved PNT capabilities.[200] They would find egregious or overly burdensome controls undesirable, which may stymie funding streams for further development, unless the technology improvement is not directly relevant to civilian applications.

[196] CISSM 2020 Report, pp. 31.
[197] "Defense Navigation Capabilities," United States Government Accountability, 2021.
[198] CISSM 2020 Report.
[199] MacKenzie, "The Soviet Union and Strategic Missile Guidance."
[200] Remarks by Deputy Assistant Secretary Hampshire, Complementary PNT Industry Roundtable, U.S. Department of Transportation, August 4, 2022, https://www.transportation.gov/administrations/assistant-secretary-research-and-technology/remarks-deputy-assistant-secretary.

Finally, because advanced PNT systems offer incremental improvements to an existing technology, not entirely new capabilities, desirability would likely also be shaped by the sheer magnitude of improvement that can be expected and the disruption potential. But, uncertainty about the pace and scale of innovation, and about what market demand for these new capabilities will actually be in the near to medium-term, will further complicate efforts to get multi-stakeholder agreement on how disruptive emergent PNT applications might be, and whether the security benefits of constraining negative forms of disruption would outweigh the enormous economic and technological costs of trying to establish some type of denial-based control arrangement.

2. Quantum Computing

Quantum computing includes computational systems that employ quantum phenomena to improve speed and/or power of operation. Compared to PNT technologies, the field of quantum computing is very young. The vast majority of organizations in this field are private companies established within the past ten years. Although quantum computing was theoretically proposed decades ago,[201] practical prototypes have only recently been developed. Because the technology is still at an early stage of R&D, there is much debate over the timescale and extent to which quantum computing could actually be achieved. However, many engineers and scientists claim that quantum computing could have wide-ranging applications in fields that require complex or data-heavy computation.[202] In the military sphere, analysts are primarily concerned about the decryption potential for quantum computers, which could theoretically render existing encryption methods vulnerable. There is also speculation about broader applications, including AI or cyber improvement and operational optimization.[203]

Quantum technologies have high barriers to market entry based on technology requirements for building quantum computers. The vast majority of organizations involved in quantum computing development are still at the early research stage; only a few companies claim to have demonstrated any small amount of quantum computing capability.[204] Given the high resource requirements that quantum computers will have in the near, medium, and long-term futures, hardware will likely remain consolidated among a small group of stakeholders, while many more organizations develop software for applications that can be run on these machines.[205]

This suggests that the proliferation risk is low and that instituting timely control policies on quantum computers and key components could not only be feasible, but also effective. Many countries have established flagship quantum programs and policy strategies within the past five

[201] Quinn Norton, "The Father of Quantum Computing," *Wired*, February 15, 2007, https://www.wired.com/2007/02/the-father-of-quantum-computing/.
[202] Francesco Bova, Avi Goldfarb and Roger Melko, "Quantum Computing is Coming. What Can it Do?" Harvard Business Review, July 16, 2021, https://hbr.org/2021/07/quantum-computing-is-coming-what-can-it-do.
[203] Kelley Sayler, "Defense Primer: Quantum Technology," Congressional Research Services, May 24, 2021, https://s3.documentcloud.org/documents/20791781/if11836.pdf.
[204] ibid.
[205] "Quantum Computing: Progress and Prospects," National Academies Press – Consensus Studies Report, 2019.

or ten years, signaling interest in the new technology.[206] Yet, the United States, Canada, and China maintain a considerable lead in developing the necessary hardware components and prototypes for quantum computing systems. Because of this lead, and the barriers to developing quantum computing hardware, countries interested in entering the quantum computing ecosystem are currently deciding whether to focus on specific components to support quantum computing research abroad, or software packages to run on other countries'/companies' quantum computers. This has led to a unique network, where countries with quantum computers, and the companies that maintain them, offer remote access or a share of access to a quantum computer to clients as opposed to directly selling a computer to make the enormous cost more economically efficient. While distributed access in some ways presents new challenges to control mechanisms, access could feasibly be restricted through working with technology providers.

Given the relatively loose connection to security applications and the high commercial sector interest, however, denial-based control policies may be detrimental to technological development and economic growth. Despite the early stage of development, the sectoral analysis found that there is already significant commercial interest in quantum computers. Within recent years, investment interest has surged for quantum technologies, indicating that investors see a variety of financially lucrative applications for quantum computing.[207] Furthermore, efforts are already underway to introduce new post-quantum cryptography standards which would effectively reduce the disruption potential for quantum computers in the national security domain.[208] This is in comparison to the enormous scientific potential for quantum computers given the early stage of development and the hype over many civilian applications that would be transformative.[209] Therefore, the economic benefits of quantum computer market accessibility could outweigh the potential security implications of wider proliferation.[210]

Quantum computing was the main technology case study where feasibility significantly outpaced desirability for controls at the present time. Given the vast commercial potential, nascent stage of development, and limited near-term military utility of quantum computing, policymakers need to decide what strategic objective should drive decisions about controls versus cooperation in this field. Some argue that the sheer scientific promise of quantum computing means that the United States government should do everything it can to innovate faster than China in order to keep, or regain, the technological lead. This would include more U.S. government funding for basic quantum information sciences R&D and more restrictions on governmental and academic technology collaborations. Others counter that this could be a good realm for using basic science

[206] Lindsay Rand, "Quantum Technology: A Primer on National Security and Policy Implications," Lawrence Livermore National Laboratory Research Paper, July 2022, https://cgsr.llnl.gov/content/assets/docs/Quantum-Primer_CGSR_LR_Jul18.pdf.
[207] Edward Parker, Daniel Gonzales, Ajay Kochhar Sydney Litterer, Kathryn O'Connor, Jon Schmid, Keller Scholl, Richard Silberglitt, Joan Chang, Christopher Eusebi, and Scott Harold, "An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology," RAND - Research Report, 2022, https://www.rand.org/pubs/research_reports/RRA869-1.html.
[208] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf.
[209] https://hbr.org/2021/07/quantum-computing-is-coming-what-can-it-do.
[210] CISSM 2020 Report.

diplomacy to improve political relations and spur technological innovation, which would make both countries safer and more prosperous over time.[211]

From a historical perspective, there is some precedent for controlling advanced computing technologies that could yield military-relevant innovations, but such policies have had mixed success in garnering support. As was discussed earlier, the United States and the United Kingdom agreed to limit exports of supercomputing technology to Eastern bloc countries during the Cold War, but disagreed on whether to restrict trade of less-advanced computing capabilities.[212] More recently, the Biden administration has also unveiled a series of controls on advanced computing chip technologies, which could provide capabilities somewhat similar to quantum processors. But these policies have also ignited concern among industry members over the economic impact from limiting access to global markets and in part due to uncertainty for the long-term security risks of such controls.[213]

3. Computer Vision

In contrast to quantum computing and PNT, computer vision is an emerging technology area where even some private sector stakeholders think additional controls would be desirable, but the feasibility of effective controls is dubious. Computer vision is a subgroup of AI technologies that includes both hardware and software components required to enable advanced image analytics. Applications for computer vision are far-ranging, and include transportation automation, manufacturing, healthcare, and surveillance.[214] However, given the capability to quickly analyze images, the defense industry is also heavily invested in computer vision applications, such as for facial recognition analysis, use in automated systems, or satellite imagery processing.[215]

The sectoral analysis found limited feasibility for policy controls, given the later stage in development and the wide spectrum of commercial applications. Specifically, the report found that most entities in the computer vision ecosystem are involved in fabrication, as opposed to R&D.[216] Elegant computer vision products are already being fabricated globally and are widely commercially available, and require minimal modification to be adapted to various applications. Compared to advanced PNT and quantum computing, this suggests that computer vision is at a later stage in technological development, and thus has fewer barriers to entry and a higher inherent proliferation potential. Additionally, in contrast to PNT technologies, the areas that are

[211] Daniel Garisto, "China is pulling ahead in global quantum race, new study suggests," *Scientific American*, July 15, 2021, https://www.scientificamerican.com/article/china-is-pulling-ahead-in-global-quantum-race-new-studies-suggest/.
[212] Frank Cain, "Computers and the Cold War: United States Restrictions on the Export of Computers to the Soviet Union and Communist China," *Journal of Contemporary History*, Vol. 40, No. 1 (2005): 131–147.
[213] Matt Sheehan, "Biden's Unprecedented Semiconductor Bet," Carnegie Endowment for International Peace Commentary, October 27, 2022, https://carnegieendowment.org/2022/10/27/biden-s-unprecedented-semiconductor-bet-pub-88270.
[214] "Computer Vision Market Research Report by Component, by Application – Global Forecast to 2025 – Cumulative Impact of Covid-19," Market Insider, July 30, 2020.
[215] "Computer Vision: Aerospace and Defense Trends," Army Technology, July 28, 2020, https://www.army-technology.com/comment/computer-vision-aerospace-defense/.
[216] CISSM 2020 Report.

more actively being developed are software components rather than hardware. As was discussed in the analysis above, software components are more difficult to control than the hardware components, which means that leaps in computer vision innovation will be much harder to control compared to those for PNT technologies.[217]

The sectoral analysis report also identified key trends in favor of desirability among the broader international community and stakeholder environment. This is despite the fact that the computer vision stakeholder environment is diverse and leans heavily towards commercial sector members as opposed to government and military members, which should decrease desirability. But, unlike the cases of the other technologies surveyed, for which companies adamantly highlighted potential negative consequences of export controls in response to the ANPRM,[218] private sector comments flagged data privacy and security concerns as drivers for their interest in control policies. Some private companies have also lobbied congress and proposed potential control policies that would address their privacy concerns.[219] Thus, in this case the scientific promise and disruption mechanisms for the technology may work in favor of desirability, even among a diverse and engaged private sector.

4. Hypersonics

Compared to the first three emerging technology sectors analyzed above, all of which are digital technologies being developed primarily by the private sector for commercial applications, hypersonic technology development more closely resembles ballistic missiles/space launch vehicles and other dual-use technologies for which national and multilateral control regimes were developed during and after the Cold War. Hypersonic technologies are most frequently discussed in the context of boost-glide and cruise missiles for military applications, particularly evading U.S. missile defenses to enhance nuclear deterrence (the most commonly mentioned Russian and Chinese rationale) and having conventional options for destroying time-sensitive targets (the dominant U.S. justification). A few countries claim to be interested in developing hypersonic capabilities for use in commercial aerospace settings, but the market case for this is very murky. This limited dual-use designation was one of the key findings of the report: unlike most of the other current emerging technologies, hypersonic technologies skew largely towards military applications.[220]

While hypersonics controls may be feasible on the basis of the technology makeup and fabrication complexity, the few countries who have been working on hypersonics for decades have had time to surmount technical hurdles. Hypersonic technologies are extremely material-intensive to produce and have high fabrication requirements, including dedicated testing facilities

[217] Mark Bromley and Giovanna Maletta, "The Challenge of Software and Technology Transfers to Nonproliferation Efforts: Implementing and Complying with Export Controls," Stockholm International Peace Research Institute, 2018, https://www.sipri.org/publications/2018/other-publications/challenge-software-and-technology-transfers-non-proliferation-efforts-implementing-and-complying.
[218] CISSM 2020 Report.
[219] IBM, "A Precision Regulation Approach to Controlling Facial Recognition Technology Exports, September 11, 2020, www.ibm.com/blogs/policy/facial-recognition-export-controls/.
[220] CISSM Hypersonic Report, forthcoming 2023.

that are exceedingly rare. But, despite the "emerging technology" label, scientists and engineers have been exploring hypersonic technologies since the 1950s, which means there has been a longer innovation period for those involved than for other truly new emerging technologies. Of those engaged in hypersonics R&D, the sectoral analysis found significantly fewer commercial entities involved than for any of the other technologies studied.[221] Instead, the vast majority of stakeholders were government/military entities or had close relations to the government/military.[222]

For this reason, the hypersonic sector survey included a country-level analysis, to account for the fact that the entities were largely contributing to government strategic interests, as opposed to universal market interests. The stage of development for the hypersonic technology sector differs markedly by country that the entities were based in, as opposed to a more normalized, global technology development pattern for the other technologies surveyed.[223] Three countries – the United States, Russia, and China – are far ahead of the rest of the world in this sector. A relatively small number of other countries have much more limited work in this area, often in partnership with one of the big three hypersonic players. In principle, therefore, *suppliers against seekers* controls would be a more feasible form of technology denial than *allies versus adversaries* approaches would be.

A realistic evaluation of the negative disruptive potential for hypersonic technologies suggests that even though recent Russian and Chinese advances have been the main motivation for increased U.S. attention to, and funding for, hypersonic cruise missile and glide vehicles, which major power has the lead in this field will probably not significantly change the strategic balance. The main motivation driving large, sustained Chinese and Russian investments in this area appears to be maintaining a credible nuclear deterrent regardless of how much progress on missile defense and conventional prompt global strike the United States might make in coming years. But, the prospect of the United States launching a disarming first strike backed by highly reliable missile defense seems unrealistic regardless of what type of hypersonic capabilities each of the Big Three has. The more worrisome strategic stability implications of hypersonic weapons development involve negative effects on crisis stability and arms race stability. These are best addressed through legally binding arms control or shared understandings about what it would mean to "compete responsibly" in this field.

Introducing hypersonic weapons into some regional security relations could be more destabilizing than adding them into the security equation between major powers that already have elaborate strategic nuclear deterrents. This creates a strong incentive to constrain proliferation to certain countries. However, because countries have diverging views on which countries controls should target based on their own unique security environments, there is not a consensus among suppliers for control parameters. One of the most significant findings of the hypersonic report is that a main mode of hypersonic technology transfer is through the establishment of military cooperation agreements between a country that has a more robust hypersonic sector and a country with much more limited capability. But it is not clear whether

[221] ibid.
[222] ibid.
[223] ibid.

hypersonic development partnerships between the United States and Australia, Russia and India, and possibly also China and North Korea are motivated more by political or economic considerations.[224] The countries with greater capabilities may be more inclined to partner with countries whose capabilities in this sector are much less robust than they are to enter intergovernmental partnerships in other sectors because lack of compelling civilian applications means the future commercial market will probably be relatively small. Thus, increased feasibility and desirability for controls in the future hinges on the United States, Russia, and China reaching some consensus on how to manage hypersonics technologies, even if they have their own unique incentives for pursuing the controls.

5. Quantum Sensing

The quantum sensing industry was surveyed in a subsequent report in order to consider connections between the PNT and quantum computing technology sectors. Quantum sensors rely on quantum phenomena to improve sensitivity and accuracy when measuring physical properties, such as electric and magnetic fields, gravitational fields, acceleration, and time.[225] Increasing PNT accuracy and durability in adverse environments is a major application referenced for quantum sensing technologies, but they also have a wider range of applications such as for imaging, communication, and basic research.[226] Importantly, because they leverage quantum phenomena, they are also very connected to the quantum computing industry and certain types of quantum sensors are even employed in quantum computing operation. Thus, similar to the PNT sector, there is a higher level of government involvement due to military PNT applications, but because of the inclusion among other quantum technologies, stakeholders in the quantum computing industry are likely to be concerned about any potential controls on quantum sensing technologies.

Like PNT technologies, quantum sensing controls may be feasible as R&D hurdles require specific materials and capabilities, and many types of quantum sensors are at an early stage of development. Unlike computer vision, or other forms of AI, quantum sensing is necessarily linked to a physical component. Depending on the type of quantum sensor, the material makeup can be challenging to acquire, or the fabrication process could require extremely precise environments and techniques. Although these requirements are not as insurmountable as compared to those for quantum computing, the feasibility for certain controls is improved by the fact that many modern quantum sensors are still at an early stage of R&D. The industry analysis found that a large fraction of the organizations involved in quantum sensing R&D were founded within the past 10 years.[227] Finally, many experts argue that the United States currently has a distinct lead in quantum sensing technology development and a handful of American companies

[224] ibid.
[225] C. L. Degen, F. Reinhard, P. Cappellaro, "Quantum sensing," *Reviews of Modern Physics*, Vol. 89, No. 035002, July 2017, https://journals-aps-org.proxy-um.researchport.umd.edu/rmp/abstract/10.1103/RevModPhys.89.035002.
[226] Michael Krelina, "Quantum technology for military applications," *EPJ Quantum Technology*, Vol. 8, No. 24, 2021, https://epjquantumtechnology.springeropen.com/track/pdf/10.1140/epjqt/s40507-021-00113-y.pdf.
[227] CISSM Quantum Sensing Report, 2022.

have produced commercially available quantum sensors.[228] Importantly, though, the sectoral analysis for this project found that many new quantum sensing companies and research groups are popping up, mostly in North America and Europe, but with some operating out of Russia, China, and Australia. Together, these factors suggest that traditional export controls could be feasible, at least in the near term before the technology development disseminates more widely and especially for specific types of quantum sensors that have higher technical requirements.

The desirability of controls on quantum sensing technologies or subcomponents is likely to be contested based on the broad stakeholder interest. While there are many defense applications driving military and government interest in quantum sensing, the level of disruption compared to non-quantum alternatives remains undefined. Furthermore, quantum sensing technologies can also be used in the civilian sphere for various activities like aerospace navigation, medical imaging, and environmental monitoring.[229] This means that stakeholders pursuing quantum sensing for civilian applications will oppose broad controls. But additionally, quantum sensing is very tightly linked with another actively developing emerging technology sector, quantum computing. Stakeholders in the quantum computing sphere may oppose controls due to the impact on their own supply chains or for the fact that they may view controls as setting a precedent for eventual controls on quantum computing technologies. This introduces another interesting control dynamic, which is the impact of linked emerging technology spheres. Given that the U.S. government issued a memo in May 2022 on the importance of maintaining leadership in quantum technologies, the impact of controls on other technologies for sustaining leadership in quantum (and other focal point technologies) is likely to be a key consideration.[230]

Insights from and limitations of the tech sector mapping exercise

As these case studies illustrate, "emerging technologies" must be disaggregated based on the technologies that contribute to or impose limits on desirability and feasibility of controls in order to better assess realistic policy options. To assess feasibility of controls, the stage of development, the technical hurdles, and the stakeholder community must all be considered, as well as the dual-use applications driving interest. Meanwhile, to assess desirability of controls, stakeholder investment, commercial applications, and mechanism for disruption must be considered. While there are trends at the aggregate level of emerging technologies for many of

[228] Edward Parker, Daniel Gonzales, Ajay Kochhar Sydney Litterer, Kathryn O'Connor, Jon Schmid, Keller Scholl, Richard Silberglitt, Joan Chang, Christopher Eusebi, and Scott Harold, "An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology," RAND - Research Report, 2022, https://www.rand.org/pubs/research_reports/RRA869-1.html.
[229] Edward Parker, "Commercial and Military Applications and Timelines for Quantum Technology," RAND Research Report, 2021, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1400/RRA1482-4/RAND_RRA1482-4.pdf.
[230] "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," United States Executive Office, May 4, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

these dimensions, each technology has unique timing or technology characteristics that may tip the scale in favor of control-oriented versus cooperative policy methods.

From the perspective of a U.S. policymaker charged with determining how strategic trade controls could enhance national security, our sectoral analysis would indicate that denial-based controls are potentially feasible for certain aspects of some technologies studied, but not others at this point in time. It would also suggest that controls on emerging technologies with clearly negative disruptive effects would be more desirable than controls on technologies with positive, disputed, or unknown disruptive effects.

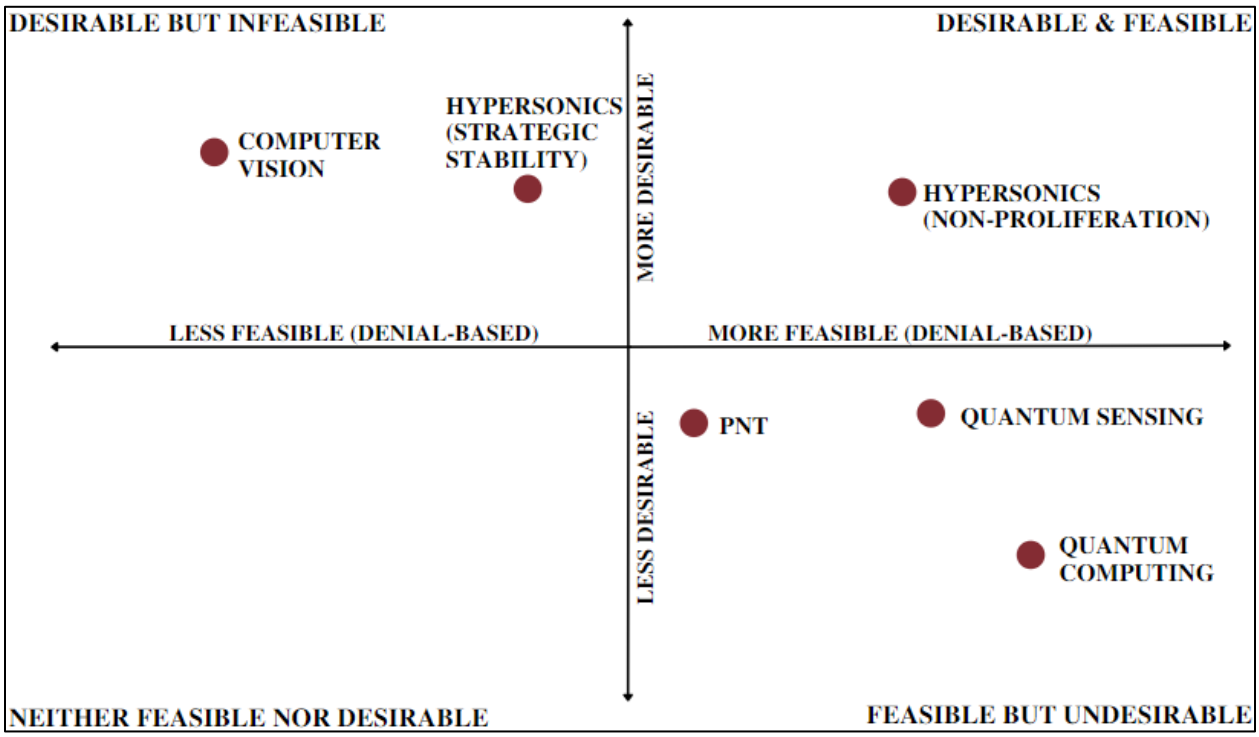
This chart depicts what such a basic assessment of the desirability and feasibility of denial-based strategic trade controls would look like. The quadrants, and positions within each quadrant, that the different technologies occupy are determined based on the sectoral analyses, with the assessment of desirability and feasibility of trade control policies for each technology visualized through their positions along the axes and indicating spectra of negative to positive desirability and feasibility estimations. To some extent, the specific positions for each technology are subjective with respect to the scope of policies considered, assessment of technology characteristics, perception of strategic impact, and inclusion of diverse stakeholder perspectives. In this chart, we indicate their locations with the specific scope of trade control policies and based on our assessment of the current state of development/dispersion, perceptions of strategic impact, and evaluation of dual-use applications and relevant stakeholders. Since others may differ in some of their assessments, this type of quad chart can be a useful mechanism for analysts and stakeholders to debate why they think strategic trade controls on these emerging technologies are more or less feasible and desirable than we have indicated.

Assuming the limited scope of a trade control policy approach, most technologies are filtered out of consideration by feasibility or desirability constraints. As a product of the technologies being selected on the basis that policymakers have identified them either as being feasible to control or desirable based on some strategic rationale, no technologies in this study fit in the bottom left quadrant, which would indicate that the technology is neither feasible nor desirable to control. Conversely, the only technology that could be both feasibly controlled and for which controls may be strategically desirable among enough key stakeholders is hypersonic technology. The caveat for the hypersonic case is that trade control policies would only be desirable from a non-proliferation perspective, in which limiting the number of countries that could acquire the technology is desirable, regardless of which countries they are.

Instead, most technologies are filtered into either the upper left quadrant (desirable, but not feasible) or the lower right quadrant (feasible, but not desirable). Although some policymakers, private sector actors, or civilians have expressed interest in controls for computer vision or hypersonic technologies, our assessment finds that controls over these technologies would be infeasible due to the high degree of dispersion and intangible components for computer vision technologies and because key actors that are likely to be the target of controls have already acquired the technology in the case of hypersonic technologies. Meanwhile, some emerging technologies like advanced PNT, quantum sensing, and quantum computing could – to some extent – feasibly be controlled for a finite period of time given current U.S. leadership, restricted

access to key materials, and R&D nascency. However, for these technologies, there is not a clear enough security risk that outweighs potential benefits of private sector development to rally key stakeholders around the desirability of trade controls.

Figure 4. Basic Strategic Trade Control Perspective



Visualizing the problem from this perspective helps explain why progress in applying new strategic trade controls to emerging technologies has been, and will remain, very slow despite the broad bipartisan consensus in the United States that tighter controls are urgently needed to widen its leadership gap in critical technologies that promise major strategic advantages. Denial-based controls are assessed to be both feasible and desirable for only one of the five technologies surveyed—hypersonics – and only if the security objective is nonproliferation. The feasibility assessment reflects technical characteristics of the sector, but political relations between the three most advanced countries are not currently conducive to a *suppliers against seekers* arrangement. If the security objective is to enhance strategic stability, the Chinese and Russian programs are advanced beyond the point where denial efforts could be very effective. Cooperative arms control and confidence-building measures would be the most cost-effective way to reduce fears of surprise attack, incentives for preemption, and arms racing. Cold war history indicates that such agreements are feasible among potential adversaries *if* they are mutually beneficial and jointly developed.

There are other reasons why this simple schematic should only be used as a starting point for thinking creatively about what types of governance mechanisms can and should be applied to

different aspects of emerging technologies. It provides only one type of stakeholder's perspective: that of a U.S. official tasked with using strategic trade controls to enhance national security. Other stakeholders could disagree about where to locate each technology because they make a different benefit/cost calculation, or think not only about chokepoints where consequential controls might be feasible in principle, but also about the practicalities of implementing such controls effectively. Placement on the chart also reflects the current state of each technology's development and diffusion; denial-based controls will be less feasible as advanced capabilities spread over time.

The "neither feasible nor desirable" cell is blank because one criterion for selecting technologies to survey was strong current demand for controls (computer vision) or being early enough in the development and diffusion process for chokepoints to still exist. AI is among the emerging technology sectors that the most powerful stakeholders would put in the neither feasible nor desirable cell, but some civil society groups are already calling for controls on certain high-consequence applications, like lethal autonomous vehicles. If a stronger consensus develops about the desirability of rules for responsible use, *cooperative management* would be the most feasible approach. Such a consensus already exists in the United States about the desirability of keeping repressive governments from using computer vision to enhance domestic surveillance. Here, also, a *cooperative management* system centered around data restriction or end-use agreements would probably be more cost-effective than any denial-based strategy for reducing the risks of misuse.

In short, findings from the tech sector mapping exercise should be used in tandem with the historical and policy analysis presented previously to stimulate more comprehensive and creative thinking about the security objectives of strategic trade controls and the reasons why *cooperative management* mechanisms might ultimately be more desirable, feasible, and cost-effective than any denial-based option.

Key lessons for policymakers

The history of technology trade controls reveals that policies based on restricting access to technologies have had mixed results in achieving security benefits even under relatively favorable circumstances. New challenges, including software-based technologies and a more globalized, private sector-driven technology development ecosystem, will further constrain the efficacy of denial-based policies for reducing risks from currently emerging technologies. Feasible control options can be identified for certain aspects of some emerging technology sectors. But even when there is broad consensus across party lines and with partner countries that about the desirability in principle of strategic trade controls on emerging technologies, getting the necessary level of multi-stakeholder agreement that the security benefits of specific feasible options would outweigh the various costs has become increasingly difficult over the decades as the United States has lost its technological lead in critical sectors, and as the relationship between government officials and private sector actors has changed. The findings of this historical and technical survey contain key lessons for policymakers tasked with trying to manage the spread and use of emerging technologies.

First, policymakers need to decide what the primary objective of strategic trade controls is. When research for this project began in 2019, the policy question posed was how strategic trade controls on emerging technologies could help reduce risks from WMD proliferation. During the second Obama and Trump administrations, though, attention in the Executive branch and Congress was increasingly moving from WMD proliferation to great power competition, especially with China. Both are important security challenges, but since China and to a lesser extent Russia are important potential suppliers of dual-use emerging technologies, it will be difficult, if not impossible, to simultaneously cooperate with them to coordinate export decisions involving countries and entities of proliferation concern, and to target *allies versus adversaries* control mechanisms against them. For example, China remains North Korea's top trading partner, and in recent years Chinese entities have supplied the North Korean government with a number of key emerging technologies, such as wireless network access.[231] Similarly, Russia's ties with Iran continue to strengthen amidst Iran's provision of UAV technology and military aid for Russia's invasion in Ukraine, sparking speculation over the technologies that Russia may provide in return, such as advanced air defense systems and hypersonic missile technologies.[232] Given the existing relationships, leveraging an *allies versus adversaries* approach is more likely to strengthen the relationships between countries of concern to U.S. policymakers in both the great power and WMD proliferation policy agendas.

Second, the historical analysis shows that, even under relatively favorable geopolitical, economic, and technological conditions, any type of denial-based control effort will be a stopgap solution at best, and is likely to have unintended negative consequences. Technology monopolies are short lived; both the Cold War and the post-Cold War analyses show that the more valuable the military advantages of U.S. superiority in some dual-use technology seem to be, the more motivated other countries will be to master that capability to anticipate and protect themselves against how the United States might use it, to demonstrate that they are also a global power, or to improve their regional security situation. By definition, *allies versus adversaries* strategies involve extensive technology transfer and collaboration between the United States and partner countries, helping the latter improve their own technological base and make export control decisions with less dependence on the United States. *Suppliers against seekers* strategies also often breed resentment, catalyzing indigenous development in countries for whom access to technology trade was restricted, counteracting the original intent of the controls. Finally, any type of denial-based control strategy has unintended negative economic, technological, diplomatic, and maybe even environmental or health effects that can generate opposition among key stakeholder groups. The more stringent the controls, the more opposition to them will grow, as evidenced by recurring cycles of U.S. export control reforms to make them tighter in an effort to increase security benefits, then less restrictive in an attempt to decrease undesirable effects.

---

[231] Ellen Nakashima, Gerry Shih, and John Hudson, "Leaked documents reveal Huawei's secret operations to build North Korea's wireless network," *The Washington Post*, July 22, 2019, https://www.washingtonpost.com/world/national-security/leaked-documents-reveal-huaweis-secret-operations-to-build-north-koreas-wireless-network/2019/07/22/583430fe-8d12-11e9-adf3-f70f78c156e8_story.html.

[232] Javad Heiran-Nia, "Iran boosts military ties with Russia in part to counteract Abraham Accords," Stimson Center Commentary, February 21, 2023, https://www.stimson.org/2023/iran-boosts-military-ties-with-russia-in-part-to-counteract-abraham-accords/.

Third, using *cooperative management* as the primary governance approach for WMD-relevant aspects of nuclear, chemical, and biological technologies has had strengths and weaknesses, too. Since this method for reducing security risks associated with dual-use technology depends not on denying access but on regulating use, there are fewer negative consequences for those who have and those who want the technology, so it should be easier to gain multi-stakeholder agreement. Moreover, because the rules are developed consensually, overall compliance should be higher than if the rules were coercively imposed, and the system should be more stable over time than if some members who have the technology and some outsiders who want it are evading controls they don't agree with. Of course, negotiating and implementing multilateral regulatory regimes takes substantial time, money, and expertise, but so does developing and running the various denial-based control systems we have surveyed. *Cooperative management* arrangements were used most extensively during the 1990s, when political relations among major players were positive, and their primary security concern involved potential threats from third parties (proliferators and terrorist groups), not from each other. But the establishment of the IAEA in the 1950s and the NPT in the 1960s shows that the United States can cooperate with a peer competitor to address a shared security challenge in a manner that is not purely transactional and that proves mutually beneficial over an extended period.

There is currently some discussion in existing *cooperative management* institutions about how emerging technologies complicate efforts to prevent nuclear, chemical, biological, and missile proliferation, but U.S. policy debates are currently focused on denial-based options for strategic trade controls. This is partly because getting broad buy-in from relevant stakeholders often requires the United States to make more concessions and compromises than if it developed the rules unilaterally or with a small group of likeminded countries, then applied them to others without their consent. During the first two decades of the Cold War and the first two decades after the Cold War, the United States had large enough technological, financial, political, and military advantages that powerful players in the Executive branch and Congress could credibly argue that the United States need not make significant concessions or compromises in order to have effective trade controls. When conditions have been less favorable for the United States to get full compliance with its preferred form of denial-based controls on dual-use technologies, powerful U.S. domestic groups have often still argued vehemently against cooperative management alternatives that might be more effective, because they objected to cooperating with countries whose leadership they abhorred, or because they opposed accepting any new legal or normative constraints on U.S. freedom to develop and use powerful dual-use and military capabilities in whatever ways it wanted.

Fourth, the historical survey shows that auspicious conditions are increasingly infrequent due to increasing interdependence, oscillating security relations among major powers, and the growing array of stakeholders and interests involved. Instead, the mix of actors that contribute to national and global technology development ecosystems and the competing interests with national security strategies based on technology restriction have made consensus on controls difficult. In these cases where there is limited consensus on controls with allies or adversaries to restrict access either through *suppliers against seekers* or *allies versus adversaries* paradigms, and where U.S. policymakers have chosen to apply unilateral controls regardless, there have been

significant economic and security consequences. In some cases, such controls have deteriorated national relations with countries that have been restricted accesses. And in the post-Cold War environment especially, such policies have imparted deleterious economic effects. In the present context, achieving consensus will be even more challenging as technology development moves further outside of the purview of the U.S. government and military, and as the prominence of economic security as a form of statecraft increases.

Fifth, the review of currently emerging technologies supports that denial-based control policies will be particularly difficult to implement effectively for long because of increasingly intangible characteristics of new technologies. The sectoral analysis of different emerging technologies underscores just how broad the stakeholder ecosystems have become, and confirms that control for most emerging technologies is not restricted or even largely driven by government and military actors. Instead, most new technologies are being developed by private industry. Of the five emerging technology sectors analyzed, hypersonics is the only case where government and military research groups are dictating technology innovation pace and focus areas. Further, each new technology has unique technical characteristics that may impact the feasibility of controls. Importantly, many new technologies have software-based components, or are entirely software-based, and thus do not easily sync with traditional control monitoring and verification regimes.

Policymakers must understand the limitations of denial-based policies in order to determine when and where they might be reasonably effective at an acceptable cost. Recognizing that controls are likely to lose efficacy over time as the barriers to technology development decrease and the relative stage of development progress suggests focusing on technologies or components that have natural barriers to acquisition dictated by hard-to-acquire materials or complex methods, and targeting technologies while the industry is relatively nascent. But as science and technology progress, these barriers will dissipate. When evaluating the strategic benefit of controls, policymakers must consider the expected duration during which the controls are likely to be effective. In the time it takes for policymakers to recognize security imperatives for governance of some specific aspect of a dual-use emerging technology, and get the stakeholder buy-in necessary to design and implement control mechanisms, technological advancement and diffusion can cause those arrangements to be outmoded, if not obsolete.

This temporal element puts a premium on having the right mix of technology and policy expertise to more quickly determine when new controls on dangerous aspects of particular emerging technologies are needed, and what approach would be both feasible and cost-effective. Policymakers need to increase capacity to evaluate and respond swiftly as concerns about the security implications of emerging technologies arise, and as new information on technology innovation and scientific potential becomes available. This requires building up in-house scientific and technical expertise, so that policymakers have sustained awareness of broad trends in technological innovation and can identify potential security risks early on. Some executive branch agencies are doing this already, and Congress should consider reconstituting something like the Office of Technology Assessment. Increasing interactions between policymakers and non-governmental experts is also important, both to help government officials make realistic assessments of potential benefits and risks associated with rapidly advancing technologies, and to help academics learn how to increase the policy impact of their expertise. It also requires

having strong advocates for cost-effective emerging technology governance arrangements inside all relevant parts of U.S. security bureaucracies and Congressional committees, plus a well-resourced and respected OST and other senior-level leadership who are committed to pushing for policy establishment quickly, rather than at a more natural pace. As one step in the right direction, the State Department has recently established a dedicated cyber and digital bureau,[233] and plans to expand its mission to encompass other emerging technologies,[234] but much more remains to be done.

Policy debates must progress beyond reiterating the need for technology policies and strategic trade controls that can restore and preserve U.S. leadership in critical emerging technologies, to determining what specific options are actually feasible, and which of those would be most broadly desirable and cost-effective. The scope of feasible governance mechanisms should be parameterized through a systematic analysis of the socio-technical characteristics of each specific emerging technology. As the five technical case studies demonstrated, each category and subcategory of emerging technology has unique characteristics that may make certain governance mechanisms more or less feasible. Technologies with critical hardware components will likely be more amenable to denial-based approaches compared to software-based technologies that can move over the internet across borders and around the world with lightning speed. Likewise, technologies with sufficiently high barriers to entry, such as quantum computers, are likely to be concentrated in a relatively small number of wealthy, technologically advanced countries. That makes them more susceptible to cartel-type control mechanisms (e.g. *allies versus adversaries* or *suppliers against seekers*), but the effectiveness of such arrangements depends on what the security objective is, whether all the countries with advanced capabilities in that area are willing to participate in a control arrangement serving that objective, and how motivated countries and entities targeted for technology denial are to circumvent and overcome those restrictions.

Policymakers need to consider a mix of stakeholders and strategic domains when evaluating the costs and benefits of pursuing whatever control options are feasible for a given technology. If a relative consensus on the desirability of controls cannot be reached among a critical group of stakeholders, then compliance problems could increase the risk and decrease the benefit of controls. Furthermore, non-military security considerations must be evaluated. Controls have and will continue to impose constraints on market efficiency that will inevitably impact U.S. R&D leadership or economic security, to some degree. The relative costs to each of these elements must be compared to the potential security benefit of controlling the technology.

U.S. inter-agency debates about how to balance security, economic, technological, and other interests affected by export controls and other technology governance options would benefit from including non-governmental and international stakeholders earlier in the process of deciding what approach would be most cost-effective. The Biden administration already recognizes the value of forming stronger international coalitions and enlisting more help from

[233] Sarakshi Rai, "State department formally launches new cyber bureau," *The Hill*, April 4, 2022, https://thehill.com/policy/cybersecurity/3258123-state-department-formally-launches-new-cyber-bureau/.
[234] Shannon Bugos, "State reviews plans for new tech bureau," *Arms Control Today*, April 2021, https://www.armscontrol.org/act/2021-04/news/state-reviews-plans-new-tech-bureau.

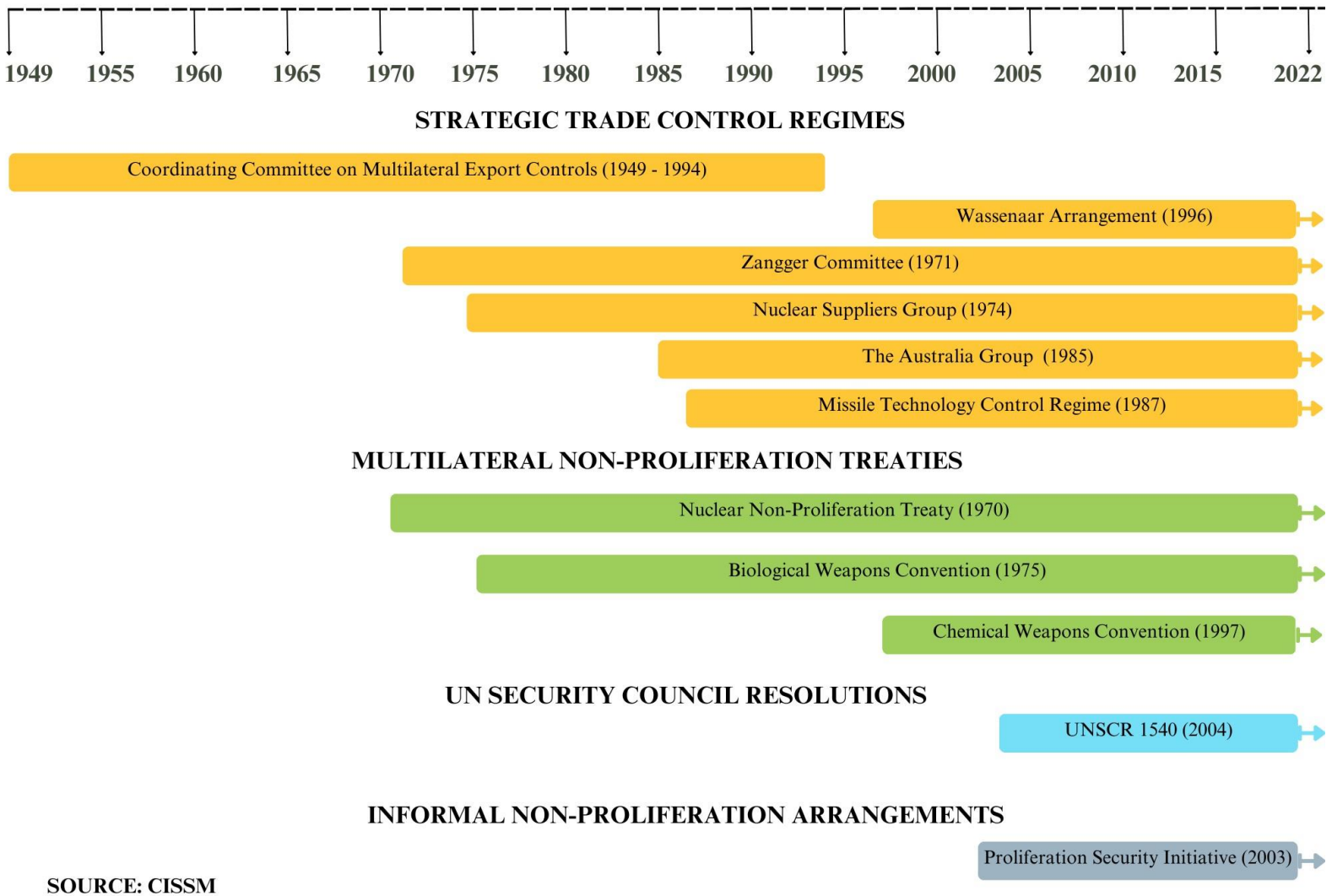
the private sector. These partners will contribute more enthusiastically and reliably if they are involved from the start in the design, implementation, and adaptation of governance mechanisms so that they remain cost-effective for all concerned as technology advances, global economic conditions change, and international security challenges evolve. Even though U.S. policymakers, foreign partners, and private sector players will often have different concerns and interests that make specific governance mechanisms more or less desirable, achieving a baseline level of consensus can improve compliance and efficacy, as has been the case in recent efforts to improve IP protection.[235]

Policymakers should expect that intangible technologies, such as artificial intelligence, or technologies with relatively low barriers to entry, such as drones and computer vision, will present vexing challenges for denial-based controls arrangements. When the desirability of controls exceeds feasibility of applying traditional methods, it could provide the impetus for an evolution in technology governance. Technologies such as lethal autonomous weapons and computer vision have been flagged by various interest groups as necessitating some form of control or governance. Yet, they do not fit neatly into existing control types. These cases will necessitate proposals for new governance mechanisms, and thus will lead to an evolution in governance methods. For example, some have proposed mechanisms to control use cases of AI rather than AI itself, or to control data rather than AI systems. Policymakers should begin pursuing research and opening dialogue on new control or governance mechanisms to tackle this.

Ultimately, as the U.S. government continues to grapple with identifying an approach to emerging technology governance, feasibility and desirability will play an important role in defining core objectives and pushing the boundaries on traditional governance mechanisms. Desirability must be assessed based on the merits of a governance mechanism in contributing to a larger strategy. And some form of consensus across relevant stakeholders must be reached to ensure a mechanism is effective. Conversely, feasibility analysis should be used to select appropriate mechanisms, and as technologies defy existing controls should be used to push for evolution in governance options. Edge cases where some types of controls are feasible, but considered undesirable by some important stakeholder groups, should be treated carefully, as preemptive controls could alter technology development or sow dissent among private sector or international stakeholders and ultimately detract from intended objectives. Edge cases where a broad consensus exists that effective trade controls are desirable, but it is not feasible to use existing control mechanisms can be an impetus to develop new governance approaches.

[235] "Recovery Through Ingenuity," United States Chamber of Commerce International IP Index, 2021, https://www.valueingenuity.com/wp-content/uploads/2021/03/GIPC_IPIndex2021_ExecSummary.pdf.

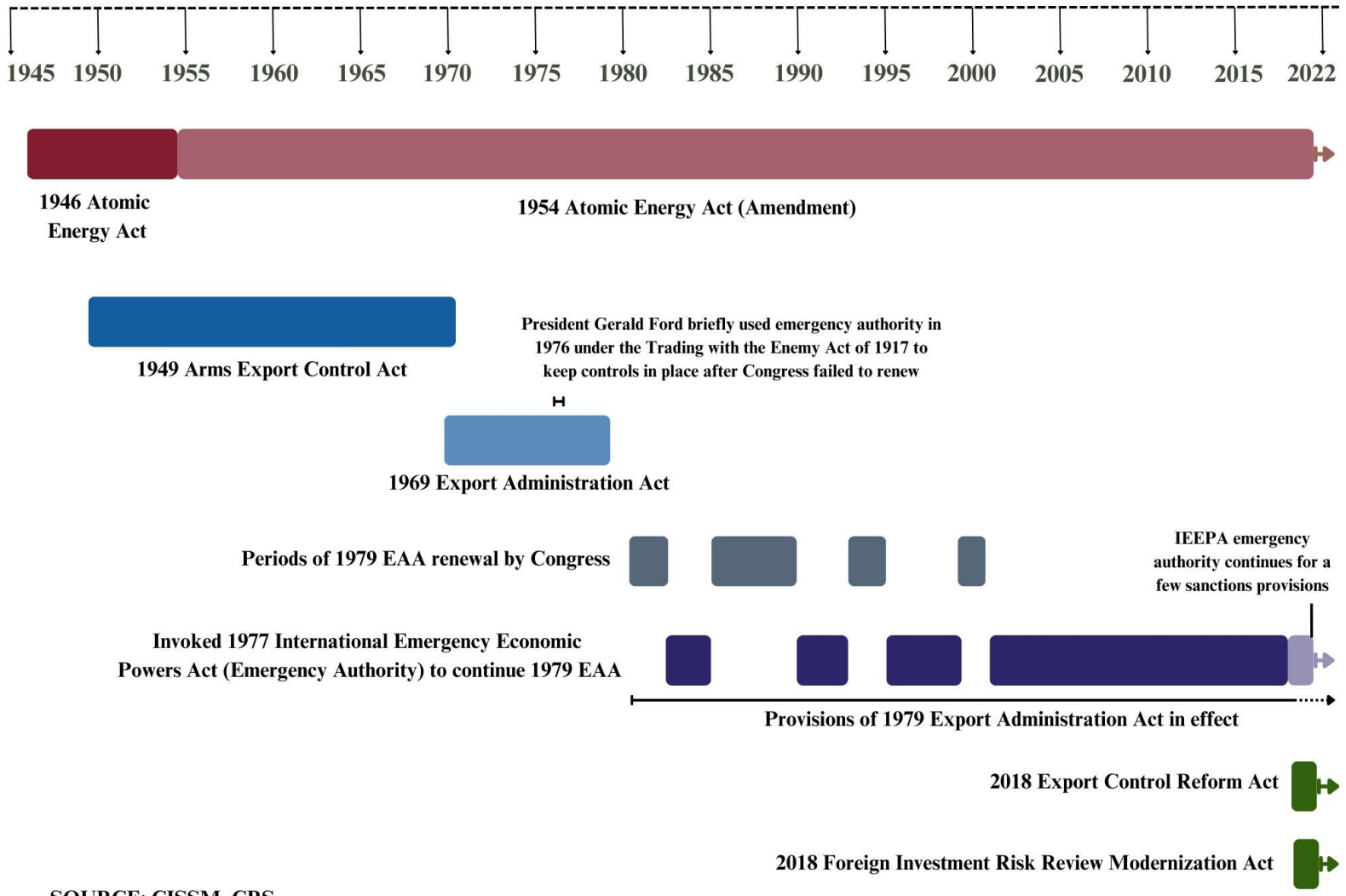
Appendix A –
Timeline of Multilateral Trade Control and Non-proliferation Arrangements



SOURCE: CISSM

Appendix B –

Timeline of U.S. Export Control Legislation



SOURCE: CISSM, CRS