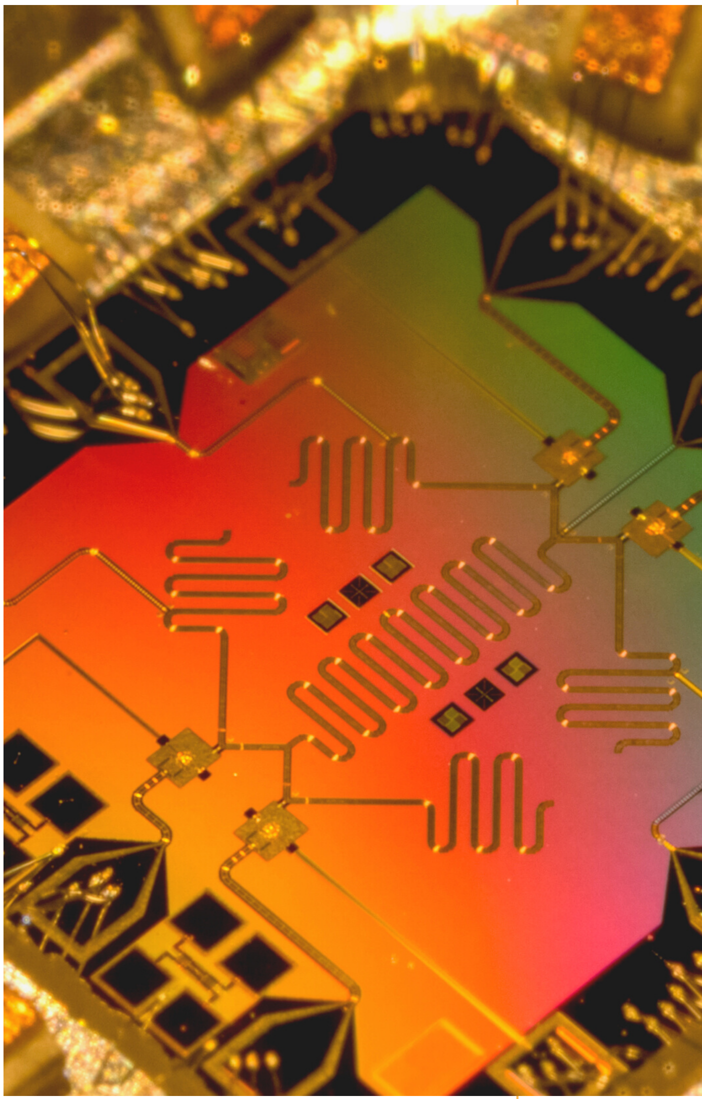
JUNE 2023

EXECUTIVE SUMMARY

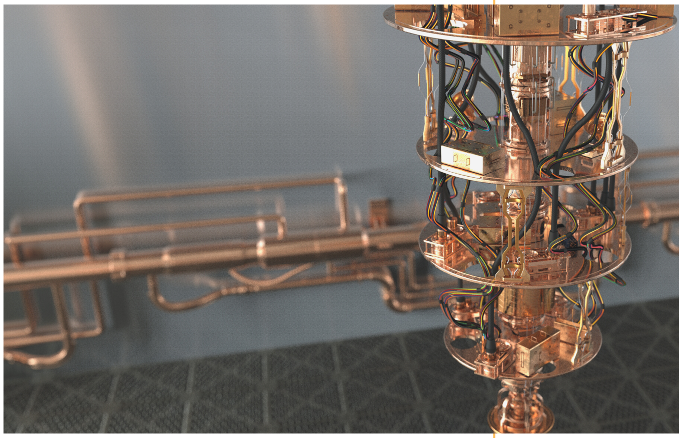
The Desirability and Feasibility of Strategic Trade Controls on Emerging Technologies



Report by:
Nancy W. Gallagher
Lindsay Rand
Devin Entrikin
Naoko Aoki

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

THE POLICY PROBLEM



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.

APPROACHES TO MANAGING DUAL-USE TECHNOLOGY

> 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.

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.

HISTORICAL ANALYSIS

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 weapons of mass destruction 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.

RECENT DEVELOPMENTS

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 artificial intelligence), 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

[1] Biden-Harris Administration National Security Strategy, October 2022, p. 3,

[2] Federal Register, Vol. 83, No. 223, Monday, November 19, 2018 (Proposed Rule) Rules

[3] "Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit," September 16, 2022,

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 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.

SOCIO-TECHNICAL ANALYSIS

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.

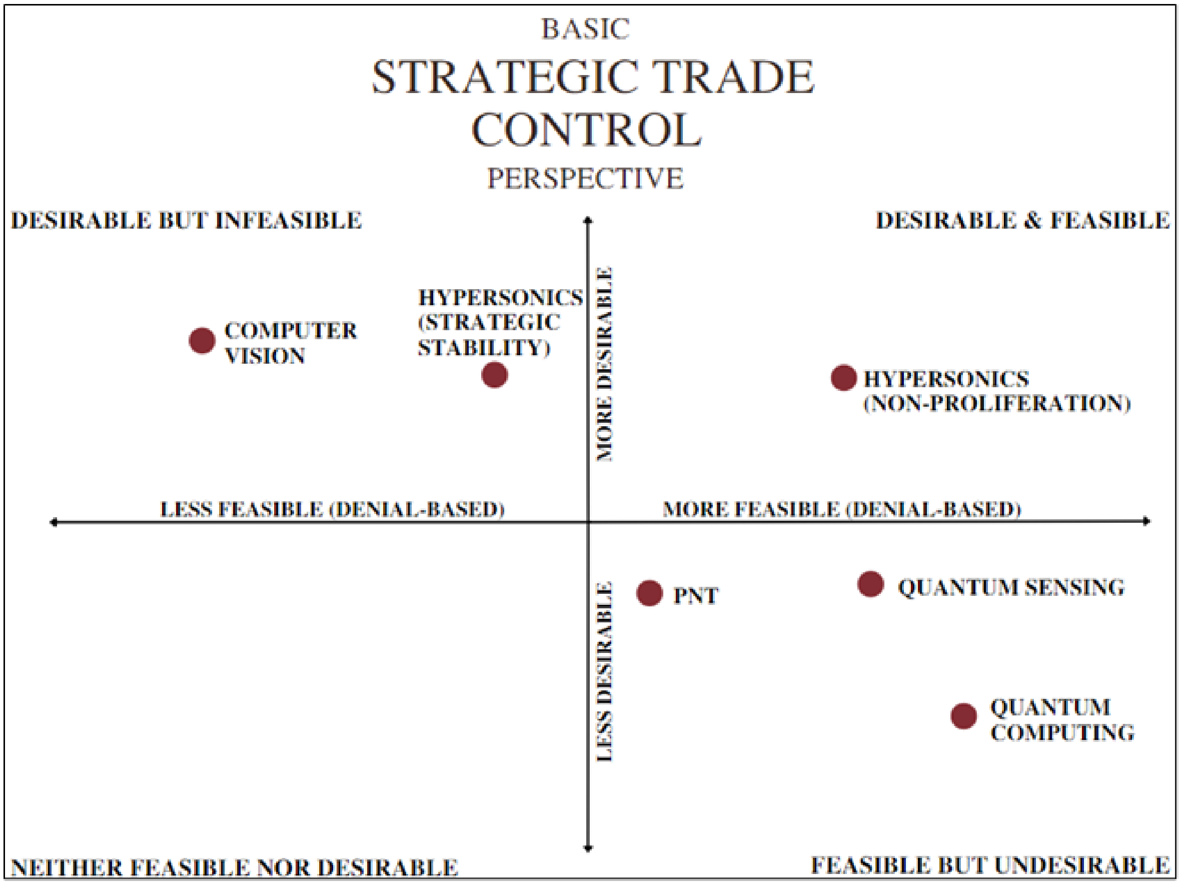
This report illustrates the importance of technology-specific considerations by summarizing key findings from a sectoral mapping exercise conducted for five technologies on the BIS list: position, navigation and timing (PNT) technologies; quantum computing; computer vision; hypersonics; and quantum sensing. 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 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.

KEY LESSONS FOR POLICYMAKERS

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.

REPORT AUTHORS

Nancy W.Gallagher, Ph.D
Director
CISSM
ngallag@umd.edu

Lindsay Rand
Research Associate
CISSM
lrand@umd.edu

Devin Entrikin
Research Associate
CISSM
dentrik@umd.edu

Naoko Aoki
Research Associate
CISSM
aoki1@umd.edu

This research was supported by the Carnegie Corporation of New York.

Download the full report

UNIVERSITY OF MARYLAND 18 56
SCHOOL OF
PUBLIC POLICY
CENTER FOR INTERNATIONAL &
SECURITY STUDIES AT MARYLAND