
***Remarks of Thea D. Rozman Kendler***
***Assistant Secretary of Commerce for Export Administration***
***Bureau of Industry and Security, U.S. Department of Commerce***
***As Prepared for Delivery***
*Geopolitics of Technology in East Asia - Stanford University - November 9, 2023*

Introduction

Good morning. Thank you to Stanford University for hosting this conference on Geopolitics of Technology in East Asia, which could not come at a more relevant time. A particular thanks to Andrew Grotto for including me in this year's iteration of this program. I appreciate your invitation because Stanford is so well positioned to bring together today's audience – professors, students, who I see as future top researchers and innovators, Silicon Valley industry leaders, and U.S. and other government officials. I welcome the opportunity to speak with you today about the transformative moment we face in geopolitics.

For those of you who do not know me, I am Thea Rozman Kendler — Assistant Secretary of Commerce for Export Administration. Within Commerce, I lead the part of the Bureau of Industry and Security that designs policy to control the proliferation of goods, software, and technology with both civil and military applications — "dual-use" items. As technologies and national security threats evolve, we identify technologies for which guardrails are necessary and amend our controls as appropriate. We screen exports, reexports, and transfers within foreign countries of technologies subject to our regulations based on an assessment of technical performance, destination, end user, and end use. Inherent to our analysis is also a careful review of any risk of diversion to unauthorized activities.

I truly welcome the invitation to address you because the intersection of technology and East Asia is a key window into the changing world we face. My Bureau is at heart a collaborative agency. We collaborate with industry in designing export controls. We collaborate with the key U.S. agencies involved in dual-use export controls — the Departments of Defense, Energy, and State — as well as the agencies deeply engaged in sanctions and enforcement activities — Justice and Treasury. Most importantly for the topic at hand, we collaborate with Allies and partner countries because only by working together can export controls be effective.

Today, I want to focus on the challenge and opportunity we face as we collaborate with our regional partners in East Asia as part of a new geopolitics of shared responsibility for developing and safeguarding the advanced technology ecosystem.

Our National Security Setting

The Bureau of Industry and Security has long focused on the challenges of *slowing* as much as possible nuclear, chemical, and biological weapons proliferation and the military advancement of adversaries, including non-state actors that might use dual-use technologies for terrorism or to destabilize countries and regions. While export controls are never airtight, I think we have succeeded in minimizing the use of U.S. technology to undermine our national security.

We recognize, however, that China and Russia – both Pacific powers – present new national security challenges.

Under General Secretary and President Xi Jinping, the Chinese Communist Party has a goal of developing the People's Liberation Army into a "world class military." He has set out to overtake the United States and our allies by dominating certain advanced technology sectors, such as artificial intelligence (AI), semiconductors and microelectronics, quantum information sciences, and biotechnology. As Commerce Secretary Gina Raimondo has observed, China poses growing challenges to our national security, including by "deploying its military in ways that undermine the security of our allies and partners and the free flow of global trade."

To fulfill its vision, China is going to great lengths to obtain key advanced technologies that are critical to military modernization. China is using all available means to modernize and advance its military with U.S. and partner country technology. It uses a military civil-fusion (MCF) strategy to deliberately blur lines between commercial sectors and military programs. This strategy is even more concerning where China's Party and government structure gives leadership the power to demand information and assistance from companies that have little choice but to agree. MCF, combined with China's governance system, has necessitated stronger export controls targeting certain commercial items that have critical military applications.

This is the challenge that my Bureau thinks about every day. We operate at the nexus of national security, technology, and global commerce. For decades, we have steadily crafted and implemented export controls, regulated our most critical dual-use items, and worked with international partners to protect our collective security.

Today, in part because of Russia's war against Ukraine, but also because of the challenges that China's actions and policies present, our work is more public. There was a time when we had difficulty even explaining our work to our parents, but now world leaders speak with fluency about our rulemaking.

Last month in *Foreign Affairs*, National Security Advisor (NSA) Jake Sullivan laid out clear principles for our relationship with China. He noted our "substantial trade and investment relationship" with China, while also describing China as a "competitor." That's the core of the complicated nature of our relationship. NSA Sullivan further shared that we do not seek to decouple, but rather to de-risk and diversify.

At the same time that we address these China challenges, Russia is bent on destroying global peace and security in its horrifying invasion of Ukraine. Relying on pariah states like North Korea and Iran for ammunition and drones, and increasingly turning to China for support, we see in Russia's attacks on the innocent people of Ukraine how naked aggression destabilizes the entire world. Export controls and sanctions have been the primary non-kinetic tools available for us to disrupt Russia's defense industry, and the challenge is even more complicated to slow China's military fusion.

The U.S. security interests in our approach are clear, and we all understand that the United States cannot go it alone. The global fissures that developed over the past few years helped embolden authoritarians seeking to capitalize on external stresses. We cannot stand by and permit — let alone facilitate — disrupters of global peace and security to have access to advanced technologies that enable globally destabilizing behavior. The rise of AI and other advanced but value neutral dual-use technologies require a new global consensus to ensure their safe application.

<u>Traditional Multilateral Controls and Partnerships</u>

As I mentioned, for over seventy years, in one iteration or another, the Bureau of Industry and Security has worked closely with partners and allies to coordinate our policies to control the spread of weapons of mass destruction and conventional weapons. This global task has been steered through four multilateral regimes—the Wassenaar Arrangement, which focuses on conventional arms and sensitive dual-use items, the Australia Group, which focuses on chemical and biological weapons controls, the Nuclear Suppliers Group and the Missile Technology Control Regime, whose names identify their objectives.

Each regime has different membership, to include countries that have the technology and capacity to contribute to proliferation. These four regimes have formal mechanisms with set annual schedules for reviewing technologies with our export control partners. They generate common control lists and common export control strategies.

For most of the world, and for many of our partners, these regimes are so intrinsic to global export control systems that their own laws only account for controls adopted via multilateral mechanisms. In some countries, domestic rules have long barred the adoption of export controls on technologies that are not part of these four regimes. On the upside, without these four regimes, many U.S. allies, including in East Asia, would not have the domestic export control authorities and rules that they have today. On the downside, the regimes can be slow and are certainly complicated by the need for unanimity.

Let me be clear — The United States remains deeply engaged in these regimes, and we continue working through them to counter the national security concerns that they were designed to address. Yet we face a problem. China and Russia belong to the Nuclear Suppliers Group, and Russia belongs to Wassenaar and the Missile Technology Control Regime. For the topic at hand, in particular, Russia has hampered the updating of controls on emerging technologies through the Wassenaar Arrangement — the group designed to address most dual-use technologies.

Emerging Technology and an Expanded Plurilateral Focus

While we remain committed to these regimes, we also recognize that the world has changed dramatically since they were set up during and immediately after the Cold War. I do not need to explain to this audience how the digital revolution complicates strategies built around the regulation of tangible goods. Advancements in science and technology mandate that we become more nimble — and more flexible — as we develop strategies more suited to both the global geopolitical context we face, and the advanced technologies of our day.

Unlike some of our allies and partners, the United States is not constrained to act only within the four multilateral regimes. When Russia launched its all-out assault on Ukraine in February 2022, we were forced to work around the existing regime system because of Russia's membership. BIS worked swiftly to bring together a group of like-minded allies and partners that includes thirty-nine major global economies. Key Pacific participants include Japan, Korea, Taiwan, Australia, and New Zealand. Together, this coalition is trying to impede Russia's ability to wage war through essentially a blanket denial on the tools and technologies essential for reconstituting and sustaining its weapon systems.

We are collectively degrading Russia's technological prowess, even while countries like North Korea try to undermine our efforts.

We understand that Russian efforts have been seriously hampered by our unprecedented level of coordinated export controls and sanctions. To be sure, Russia is desperate for workarounds. Yet it is also important that the technologies we — and our allies and partners — innovate are not being used to massacre Ukrainian civilians or to pursue imperial wars of aggression. Given that some of the products our companies make are digital and very small, and given that there are many legacy items — even recycled items — that are useful in Russia's weapons and the drones Iran makes for Russia — the challenge of keeping our goods out of the Russia war effort is formidable.

Over time, particularly with the joint leadership of the European Union, Japan, the United Kingdom, and the United States, we have expanded the items we are denying to Russia and are working to stop the transshipment of goods that aid Russia's war effort. This fall, we agreed on and publicly released a list of 45 Harmonized System codes covering the microelectronics and other items of military significance sought by Russia and Iran for missiles and drones. And we have jointly shared our "Common High Priority Goods List" with other countries, leveraging a shared concern around the world. Just two weeks ago in Kuala Lumpur on the sidelines of the Southeast Asian Forum on Export Controls, I shared the List in separate meetings with 14 governments, and my Japanese counterpart presented it during his plenary keynote address.

I mention our Russia wartime efforts because these international efforts – outside of the traditional export control regime environment – are fundamental to BIS's approach to modernize export controls. Technology supply chains span across borders, and technological expertise is dispersed throughout the world. The best way to truly keep potentially dangerous technologies and know-how out of the hands of bad actors is to work together. Coordinated controls reduce instances of evasion or backfill by other suppliers from other countries, ensuring that our controls remain effective over the long term.

Of course, there are rare cases where the United States truly monopolizes production of a critical technology to the extent that unilateral controls can be effective. Those of you in industry know that these areas of unilateral dominance are fewer and far between than some policy makers may imagine. You also know that technology keeps leapfrogging ahead. We may be dominant today, but this does not mean that our technology will be dominant tomorrow. "Damming half the river" by imposing export controls when other manufacturing countries do not will not accomplish our national security objective.

Which brings us to another challenge: We cannot hinder U.S. exports only to create a market opportunity that firms based in other countries quickly fill. In this respect, unilateral export controls are most likely to result in an unlevel playing field for U.S. industry. So, while there is a place for unilateral controls, particularly when mandated by U.S. values, acting alone is not the preferred approach.

I should note that this understanding of limits of unilateral strategies goes back decades. We learned this lesson during the Cold War, and for over fifty years the Bureau of Industry and Security has been instructed by statute when we impose new controls to prioritize multilateral strategies and to consider whether an item is readily available from suppliers in other parts of the world.

In this difficult moment, we are fortunate to have vibrant export controls partnerships, particularly in East Asia. Under Japan's leadership, in the May 2023, G7 Hiroshima Leaders' Communiqué, leaders reaffirmed that export controls are "a fundamental policy tool to address the challenges posed by the diversion of technology critical to military applications as well as for other activities that threaten global, regional, and national security." The leaders further noted the "importance of cooperation on export controls on critical and emerging technologies such as microelectronics and cyber surveillance systems to address the misuse of such technologies by malicious actors and inappropriate transfers of such technologies through research activities." This statement demonstrated a seminal moment in strategic controls collaboration.

Applied to the China threat, these principles drive our calibrated and targeted approach. China has tried to characterize U.S. export controls on advanced semiconductor production, supercomputing, and artificial intelligence as an economic measure aimed at restraining its economic growth. Restraining technological development and growth is not our goal. Let me repeat: Our goal is *not* to decouple from China. Our goal is *not* to hinder China's economic development. Our goal *is* to use a scalpel approach to hamper China's military modernization efforts by restricting key, sensitive technologies.

The Bureau of Industry and Security's placement in the Department of Commerce is by design. Commerce is especially sensitive about the need for U.S. technological leadership. We know that Silicon Valley — its industries and research centers — collaborates with international partners. And we know that U.S industry needs to take advantage of global scientific collaboration and global markets. This knowledge means that we need to carefully control the export of the most sensitive items to entities and activities that threaten our national security.

We need to impose controls intelligently, without unduly interfering with critical research or commercial trade that doesn't undermine our national security.

Let me speak specifically about our export controls vis-à-vis China. We recognize that China's efforts to develop and employ advanced artificial intelligence in its military modernization demanded a clear and proactive export controls strategy. Last year, and in updates just several weeks ago, the Bureau of Industry and Security released new controls restricting China's access to critical advanced computing items and supercomputing capability. Our goal is to restrict access to advanced chips that can support critical artificial intelligence applications with a national security nexus, and semiconductor manufacturing equipment that can aid China's advanced chip development.

I don't think I need to explain to this audience just how important artificial intelligence is to military modernization. We've heard artificial intelligence described as the "quintessential" dual-use technology. The bottom line is that artificial intelligence capabilities—facilitated by supercomputing, built on advanced semiconductors—present U.S. national security concerns because of their ability to dramatically approve military capacity. Nevertheless, we know artificial intelligence also provides tremendous potential for civil applications, including life-saving medicine.

These targeted controls are not multilateral. We do not yet have consensus for our advanced chip and semiconductor manufacturing equipment controls through a formal multilateral regime. Because we have a deep national security concern stemming from the misuse of an emerging technology, we could not wait. While we prefer to work multilaterally, we will not hesitate to act unilaterally to protect U.S. national security.

Other countries that produce the most advanced semiconductor manufacturing equipment have adopted similar controls under their national regulations. And we are working on multilateral or plurilateral controls to address advanced semiconductors. Even when fabricated outside the United States, such as in Taiwan, the advanced chips controlled under our regulations are the direct products of U.S. tooling and software. Accordingly, under our Foreign Direct Product rules, we have unique control over this technology even without other countries joining us for now.

We're working hard to ensure that our unilateral controls do not have unintended spill-over effects. Along with our updates to the advanced chips and semiconductor manufacturing equipment controls last month, BIS also issued a rule updating our general authorizations for key Korean semiconductor firms—namely SK Hynix and Samsung—operating fabrication facilities in China that support these companies' worldwide operations. Samsung's and SK Hynix's fabs in China are Validated End-Users (VEUs), a term in our regulations that is applied to specific facilities that have undergone a national security review and obtained approval from the U.S. government to receive certain items that otherwise would require licenses. Our action was critical for the ongoing prosperity of our global semiconductor supply chain and ensures that this supply chain remains as secure and transparent as possible.

Speaking of Korea, I have great hopes for the U.S.-Korea Supply Chain and Commercial Dialogue – SCCD —Dual-use Export Controls Group that I launched in Seoul one year ago. Building off of the work led by Secretary Raimondo and her Ministry of Trade, Industry and Energy (MOTIE) counterpart, we are using this Working Group to enhance collaboration and ensure that our use of export controls is consistent with the promotion of bilateral trade and the stability of the global supply chain in advanced manufacturing, as well as to share best practices and information and to increase stakeholder engagement and support across government, industry, and civil society.

Similarly, we maintain close contact with our counterparts in Japan through the JUCIP – the Japan-U.S. Commercial and Industrial Partnership. In the Second JUCIP Ministerial Joint Statement, released in May, we reaffirmed our commitment to aligning on Russia controls, including by addressing circumvention and backfill efforts, conducting capacity building and outreach within Southeast Asia and with other third countries, and implementing actionable recommendations received from the public.

Our partnerships with both Japan and Korea, which run quite a bit deeper than just these activities, are key to fostering trusted technology ecosystems, combatting economic coercion, and preventing the misuse of sensitive technologies to undermine our national security and the security of our partners and allies.

Our collaboration with Japan and Korea colleagues has also helped us navigate our relationships in Southeast Asia. This region is increasingly positioned as a reliable and responsible contributor to the development of the world's most critical technologies. We hear from multinational corporations just how important Southeast Asia is to their diversification and de-risking plans.

In manufacturing, we are seeing countries including Vietnam, Malaysia, and Thailand emerging as key players in global technology supply chains. Malaysia, for example, has played a crucial role in the diversification of the global semiconductor supply chain, with international companies like Infineon, Intel, Texas Instruments, and others announcing plans to invest and expand across the country.

The Indo-Pacific Economic Framework for Prosperity (IPEF), as well as bilateral initiatives on critical and emerging technology, also present key opportunities in the region. While these activities and fora are not centered around export controls, their focus on transparent, diverse, secure, and sustainable supply chains complements our efforts to develop new strategic trade approaches.

We are transparent in identifying our national security concerns and their direct connection to our export controls. We make public our lists of controlled technology, entities that are barred from receiving technology without a license, and entities that are sanctioned for export controls violations. We also make public the policies that we in the government apply as we review license applications. The "small yard, high fence" approach – noted by NSA Sullivan in his article – requires us to be clear to all about what we are protecting behind our fence. We have been consistent: the same advanced technologies that receive extensive attention in export controls are the subject of the Outbound Investment Executive Order – semiconductors and microelectronics; quantum information technologies; and artificial intelligence. The Biden-Harris Administration recognizes that in the globalized advanced technology ecosystem we must have open and clear dialogue about the security threats we face, including those posed by China and Russia.

## Conclusion

Trade and technology are poised to provide massive benefits to human progress and innovation, and we must maximize these collective benefits for governments, companies, workers, and citizens around the world. At the same time, these technological discoveries present adversaries and bad actors with new opportunities to improve their militaries and weapons systems. We cannot be naïve. Some technologies that can be used for good can also be weaponized in the wrong hands. This means that tools like export controls are more important than ever in balancing the risk and benefits of dual-use technology. New strategic trade control tools are essential to combatting the spread of software, technology, and know-how that enable actors who would use them against us and our partners.

We are working through existing regimes and building new plurilateral and bilateral engagements with crucial partnerships. Our partnerships in the East Asia region are critical to the strategy's success. Together, we face a need for new global approaches to strategic trade. We all have a role to play in ensuring that the fruits of advanced technologies are applied to our shared security and prosperity.

We believe in the power of multilateralism over unilateralism whenever and wherever possible. We believe that U.S. policy is more effective when it is crafted with input from industry involved in creating new technologies and developing new markets. U.S. export controls have and will always be most effective when deployed in conjunction with those of governments and firms that share our values. As technology evolves, we will have a stronger response if we are coordinated with our closest allies and as we continue to work towards a shared vision of global security.

Thank you.