WILLFUL BLINDNESS:

AN INSIDER'S ACCOUNT OF HOW AMERICA'S INEFFECTIVE EXPORT CONTROL REGIME INCREASES CHINESE MILITARY STRENGTH

MAY 10, 2023

BY STEPHEN COONEN, CHINA TECH THREAT SPECIAL ADVISOR



TABLE OF CONTENTS

FOREWORD FROM THE AUTHOR
EXECUTIVE SUMMARY
CHINA'S MILITARY-CIVIL FUSION POLICY: RENDERING U.S. EXPORT CONTROLS IRRELEVANT
THE U.S. GOVERNMENT RUBBER STAMPS TECHNOLOGY TRANSFERS TO CHINA
HUAWEI AND SMIC EXPOSE INEFFECTIVE U.S. EXPORT CONTROL POLICIES
6 FLAWED RATIONALES FOR APPROVING CHINA-FOCUSED LICENSES
8 RECOMMENDATIONS FOR STRENGTHENING EXPORT CONTROLS TO DEFEND SENSTITIVE TECHNOLOGIES
CONCLUSION
ENDNOTES

FOREWORD FROM THE AUTHOR



Receiving the Superior Civilian Service Award



Graduating from the National War College

Following more than two decades in uniform as a U.S. Army artillery and foreign affairs officer, I spent nearly fourteen years as an analyst at the Defense Technology Security Administration (DTSA), the Pentagon's unit for developing export control and technology security policies. I worked with many outstanding colleagues across the federal government to prevent American technologies from falling into the hands of our most dangerous adversaries. By the end of my tenure, I was the DTSA's Senior Foreign Affairs Advisor for China, a nation which virtually all military and civilian national security analysts today regard as the United States' pacing threat. In this position, I helped protect America from Chinese attempts to obtain sensitive American technologies that can be directed against our own military personnel. I had the privilege of writing memos for the Secretary of Defense and other senior leaders. I graciously received bonuses tied to my work. I won top performance awards, including the Award for Excellence from the Office of the Secretary of Defense in July 2020 for my work on China.

In November 2021, I voluntarily resigned in protest from my post.

The reason for my resignation was rooted in both principle and policy: I had exhausted my ability to positively influence DTSA leadership to be more aggressive in denying the transfer of American technologies to China, which our enemies in Beijing have no doubt diverted for military purposes. I could no longer in good conscience continue to serve leaders who refused to recognize and correct U.S. export control policy failures concerning China.





Retiring as a Lieutenant Colonel

respect for virtually all of them remains high. My sole motive is to speak out against a broken system in hopes of reforming it. American export control policies are completely failing to stop the transfer of militarily useful American technologies to China. I also write this paper out of respect for the brave and honorable Americans who still wear the uniform. I spent my career supporting the greatest fighting force the world has ever seen: the U.S. military. To see how our export control policies continue to feed the buildup of an adversarial Chinese military is to watch a car crash unfold in slow motion. The nominally civilian technologies American companies are permitted to sell to China today could be leveraged to kill American military personnel in the Pacific tomorrow. As I will demonstrate, a willful blindness among various actors participating in the regulation of technology sales to Chinese entities characterizes our export control system. This negligence undermines American national security and dishonors our forces' willingness to sacrifice for our country.

For these reasons, I have written this paper to expose the defective aspects of U.S. export control policy and recommend solutions for fixing them. I do not pretend that the necessary overhaul will be easy. Bureaucratic inertia, an overly legalistic perspective on the problem inside the federal government, and commercial interests' advocacy against common-sense national security policies all stand in the way of meaningful reforms. But those reforms are more necessary than ever.

The Chinese Communist Party is the greatest external challenge to American power of our time. How we respond will shape the world our children and grandchildren live in. My humble hope is that officials with power to revise the export control system in ways that meaningfully protect American national security will do so.

Stephen Coonen

May 2023

EXECUTIVE SUMMARY

Although the United States has come to recognize myriad security threats posed by China, the United States Government has yet to fully recognize, or admit, how its own insufficient technology transfer and export control policies are strengthening the Chinese military. Far from restricting key technologies, U.S. export control policies are certainly permitting U.S. companies to supply the People's Liberation Army (PLA) with the very capabilities that could be deployed against the United States in a future conflict. Chinese assurances that American technologies licensed for civilian uses inside China will be confined to those purposes are worthless in light of the Chinese government's state-led Military-Civil Fusion (MCF) program and serial dishonesty. China's exploitation of the current export control regime makes a mockery of U.S. controls, increases the strength of the Chinese military, and endangers the American warfighter.

The U.S. government must amend ineffective policies by implementing the following solutions:

1. <u>Eliminate a general policy of approval, and make a presumption of denial policy the default position</u> <u>for National Security (NS)-controlled technologies bound for the PRC</u>

Per the Export Administration Regulation (EAR), technologies that "make a significant contribution to the military potential" of a country are controlled for national security reasons.¹ The United States should not be in the business of transferring technologies that make a "significant contribution to the military potential" of the PLA, especially in light of China's MCF strategy to divert foreign technologies and no effective verification mechanism for how those technologies are used inside China in place. There should be no general policy of approval and the presumption of denial policy for NS-controlled exports destined for the PRC should be the top-line position regardless of the alleged end-use.

2. <u>Establish and immediately enact a presumption of denial policy for specific critical technologies</u> <u>destined for the People's Republic of China (PRC)</u>

BIS must have a broader consideration of how China is making use of American technologies for military purposes. Licenses for the export of certain key technologies to China should be automatically denied. These exports should include specific types of integrated circuits, key gas turbine engine technologies, certain composite materials, and technologies used in the development of hypersonic engines, all of which have meaningful military applications and relatively low foreign availability. There are invariably other critical technologies upon which the CCP is dependent to achieve their vision of global domination and where there is little foreign availability that the U.S. government should similarly deny.

3. <u>Give the Departments of Defense, State, and Energy greater authorities to influence the outcomes</u> of license reviews for controls where they have the largest equity stake

The Commerce Department's Bureau of Industry and Security's (BIS) track record of rubberstamping export licenses should prompt Congress to reassign final transfer decision authority over commodities controlled for national security reasons to the Department of Defense. Similarly, the Department of State should have greater authority over commodities controlled for regional stability and some of the multilateral non-proliferation controls. Nuclear technologies should be largely the domain of the Department of Energy.

4. Revise timeline requirements for transfers to the PRC

The federal government currently has 30 days to review transfer requests to China. This time period is inadequate. The federal government should be allotted additional time, e.g., 90, 180, or 365 days, to review proposed exports. The additional time will permit more meaningful analysis of potential military applications, give the intelligence community more time to research potential end uses, and provide export control officers with additional time to conduct pre-license checks.

5. <u>Congress should direct the Administration to renegotiate the U.S.-China End-Use Check (EUC)</u> <u>Agreement</u>

The principle of the Russian proverb "trust, but verify," should undergird a renegotiated U.S.-China End-Use Check Agreement. As the agreement stands currently, it affords the U.S. no effective means to confirm actual end-use or end-users in China. Until such an updated agreement is achieved, it is wholly irresponsible for the U.S. government to continue to approve the transfer of militarily useful technology to the PRC.

6. <u>Afford the interagency bodies overseeing export control a greater ability to establish controls for</u> <u>unlicensed and emerging technologies</u>

Transfers of technology requiring a license are just a fraction of the total amount of militarily useful technology transferred to China every year. Technology that is not subject to U.S. export controls is also a significant resource for China's military modernization efforts. BIS leads the interagency effort to add and remove technologies from the Commerce Control List (CCL). BIS is often sluggish in establishing controls for emerging technologies and increasingly unilaterally declares certain commodities to no longer have licensing requirements. Congress should expand the authorities of the Departments of Defense, State, and Energy to facilitate their ability to establish controls on the CCL for technologies where the reasons for control fall primarily under their purview.

7. <u>Work with key partners and allies to resurrect a multilateral export control regime similar to the</u> <u>former Coordinating Committee for Multilateral Export Controls (COCOM)</u>

The four primary multilateral control regimes are ineffective in implementing needed restrictions or adding additional meaningful controls in a timely manner, if at all. As the U.S. implements more consequential export control policies vis-a-vis the PRC, it should work with select like-minded international partners to avoid the pitfalls of unilateral controls and to establish a new multilateral export control regime similar to COCOM that is better equipped to deal with the rapidly changing realities impacting international security.

8. Congress should order a GAO audit

BIS has a history of unilaterally disregarding Department of Defense (DOD) conditions, determining licenses are not required during reviews without consulting other stakeholders, and ignoring interagency requests and conditions for adding non controlled or emerging technologies. Congress should order a Government Accountability Office (GAO) audit to access the extent of BIS disregard for regulatory authorities and access the risk to national security caused by violating established procedures.

CHINA'S MILITARY-CIVIL FUSION POLICY: RENDERING U.S. EXPORT CONTROLS IRRELEVANT

China, the United States' foremost strategic adversary, will go to nearly any length to acquire the technology that it needs to realize its economic and military ambitions. While China's widespread theft of American technologies is by now well known, too few Americans understand that the United States indirectly assists China's military modernization efforts through the authorized export of controlled technologies such as software, microelectronic components, or technical data, to name a few examples.

While the U.S. has long had export control laws on the books designed to ensure American technologies do not enhance competitors' military capabilities, the current set of rules have proved ineffective. In 2021, the U.S. Commerce Department's Bureau of Industry and Security (BIS) approved 88% applications for the export of controlled technologies to China, only marginally better than 2020's 94% rate.²

APPLICATIONS FOR U.S. EXPORTS OF CONTROLLED TECHNOLOGIES TO CHINA, 2021



Many technologies subject to export licensure are "dual-use" in nature, i.e. they have both civilian and military applications. For example, the seemingly innocuous carbon fiber filament used to make high-performance brake pads is also the same material used to manufacture nose cones for ballistic missiles. Field programable gate arrays (FPGAs) can be used in an array of telecommunication devices, such as cell phone towers or in advanced military radars. BIS, with the consent of other federal agencies, approves exports to China at high rates because both American companies and Chinese entities claim that the technologies in question will be used strictly for civilian purposes. On the American side, these claims are rooted in willful blindness as to China's intentions and capabilities. Chinese entities are simply lying.

Despite the U.S. government's nominal measures for verifying end-uses, there is no reliable way to prevent technology acquired by the PRC's "private sector" (there is no true private ownership of property in China) from being diverted to the PLA. While voluntary research partnerships between militaries and private organizations are common in the U.S., no U.S. government entity can compel a private organization to share its intellectual property with the military. That is not the case in China. China's National Security Law, Cybersecurity Law, and National Intelligence Law provide CCP officials

with the despotic authorities to redirect imported controlled technologies to the PLA, the Ministry of State Security (MSS), or wherever the capability can be best utilized. This policy of Military-Civil Fusion (MCF) is a state-led program overseen by Xi Jinping himself, and is designed to build up Chinese science and technology knowledge across military and civilian sectors.

Hence, where prohibiting American technologies from getting into the PLA's hands is concerned, the PRC's MCF strategy renders the current U.S. export control regime completely impotent. Under MCF, any technology transferred to China's civilian sector, to include intellectual property derived from business deals with U.S. companies, can be co-opted by the Chinese military. No matter what a Chinese entity declares the <u>stated</u> end use of an American technology to be, it is impossible to know the <u>actual</u> end-use purpose or end-user.

THE CHINESE GOVERNMENT'S OPACITY

The Chinese government is distinguished by a lack of transparency. On May 1, *The Wall Street Journal* reported on the Chinese government's growing willingness to restrict economic information from foreign companies doing business in China:

Prodded by President Xi Jinping's emphasis on national security, authorities in recent months have restricted or outright cut off overseas access to various databases involving corporate-registration information, patents, procurement documents, academic journals and official statistical yearbooks.³

One example in which China's MCF strategy has paid dividends is in its well-documented leap in hypersonic missiles. China's hypersonics sector has benefitted from American technology, much of it derived from U.S. tax-payer funded military research. Chinese firms which are not on the Entity List have spent years purchasing American technologies to hand over to the Chinese military. A 2022 *Washington Post* report found that, "Scientists who work in the sprawling network of Chinese military research academies and the companies that aid them said in interviews that American technology – such as highly specialized aeronautical engineering software – fills critical gaps in domestic technology and is key to advances in Chinese weaponry."⁴

Such deception is only a glimpse of how Beijing intends to leverage any American technology of value for military purposes. But the MCF policy is not the only reason to doubt China's intentions for American exports. Underlying the entire concept of export controls is the principle of trust – whether the U.S. can have confidence in a foreign government not to violate the terms of a technology's use. Many officials responsible for U.S. export control policy take the Chinese government's declarations of what technologies will be used for at face value.

But the Chinese Communist Party is characterized by dishonesty: one only need look at its lies regarding COVID-19, their broken promises not to militarize the South China Sea, violated treaty obligations regarding Hong Kong, denials of abusing ethnic minorities in Xinjiang and Tibet, and most recently, claims that a surveillance balloon loitering above U.S. strategic missile sites was only an errant weather balloon. Why do U.S. export control officials imagine that these same leaders will honor end-user conditions for technologies that the PLA and MSS need?

THE U.S. GOVERNMENT RUBBER STAMPS TECHNOLOGY TRANSFERS TO CHINA

Despite the PLA's continued buildup, China's MCF strategy in facilitating it, and the CCP's dishonesty, the U.S. export control system continues to provide the PLA with militarily useful U.S. technologies.

Even the most recent attempt to update Section 742.4 of the EAR concerning national security controls of technology to reflect China's MCF strategy was an utter failure. According to the EAR, NS controls are intended to "ensure that these items do not make a contribution to the military potential" of certain countries – most promanently China. The revision added a "presumption of denial," for exports that would make "material contributions" to those states' military capabilities – which is essentially already established in the control itself.⁵ Export control officials then willfully ignored the CCP's MCF strategy by citing a "general policy of approval" for technologies being obtained by Chinese end users claiming civilian status, as is lawful under Section 742(7)(i) of the EAR. Thus, a revision that was designed to account for China's systematic and very public policy of diverting U.S. technology to its military has had no impact. I personally recall that, as of August 2021, U.S. government statistics on U.S. exports to the PRC revealed that the U.S. government was approving more than 95% of national security-controlled technology transfer requests. There is little reason to think that number has meaningfully changed since that time.

China is able to legally appropriate so much American technology because various federal agencies inadequately considering national security in the license review process. The review and adjudication of controlled technology is an interagency process led by the Department of Commerce, whose senior decision-makers are preponderantly influenced by industry voices advocating against tighter export controls. Other stakeholders include the Department of Energy, the Department of State, and the Department of Defense (DOD). Each federal agency participating in the review process is permitted to challenge licensing decisions.

DOD plays a crucial role in the export control process in conducting national security assessments on the export of militarily useful U.S. technology. One would think DOD would instinctually refuse to approve exports of national security-controlled items, or any technology of military utility. Sadly, DOD often inexplicably choses to downplay national security implications in China-related interagency transfer decisions, and instead routinely acquiesces to BIS. In fiscal year 2021, only 57 transfer decisions out of 41,000 license applications were referred for higher-level scrutiny – and several of these challenges were not China-related.⁶ These statistics reveal that the current export control system is skewed to advance industry interests. Even worse, it shows that the Pentagon is failing in its primary mission of maintaining the American warfighter's fighting edge.



3 WAYS BIS SIDELINES OTHER FEDERAL AGENCIES IN THE EXPORT CONTROL REVIEW PROCESS

Bureaucratic obstinacy at BIS plagues America's export control regime:

- 1. Commodity Classification: As it stands today, BIS oversees commodity classifications the process of determining which technologies are controlled. Although BIS regularly requests input from interagency officials on which technologies should be controlled, BIS officials routinely ignore their recommendations. Nor is there a dispute resolution mechanism for disagreements on the classification. BIS is the final arbiter in deciding what is and what is not controlled, and their equities placating American firms eager to sell to China are not aligned with DoD's equities: national security. Consequently, there are technologies and capabilities that engineers at DoD believe should be controlled but are not, such as certain additive manufacturing capabilities or specific integrated circuits.
- 2. License Reviews: The Departments of Defense, State, and Energy have the authority to review any export license application submitted to the Department of Commerce. Yet BIS is known to return export applications to the applicant stating a license is not required while these agencies reviews are underway, and without coordinating with them.
- **3.** Conditions for the Export of Controlled Technologies: Export control authorities will often approve transfers but add requirements or restrictions to protect against unauthorized use and mitigate risks of diversion. BIS habitually does not inform applicants of these risk mitigation requirements or restrictions as conditions for approving transfers. With the elimination of DOD conditions from export licenses, BIS is negating DOD's national security concerns.

DOD export control leaders' timidity in confronting their BIS counterparts on these process fouls seems to have merely emboldened BIS' brazenness.

Under such circumstances, a Government Accounting Office (GAO) audit of the export control process is fully merited to shine a light on the extent of the problem. But no one should expect any action if the Department of Commerce is directed to execute such an audit. Even as far back as 2002, a GAO inquiry into China's advances in the semiconductor industry noted that the PRC was rapidly closing the capabilities gap in semiconductors. The GAO identified a weak Wassenaar Arrangement mechanism for multilateral controls, cited a general licensing policy of approving applications (except those items that would make a direct and significant contribution to specific areas of China's military), and stated that there was no interagency analysis of the cumulative effects of such exports on U.S. national security interests.⁷ These problems persist today, and are even more pressing than they were more than twenty years ago as the world sees Chinese advancements in semiconductor manufacturing and the PLA's modernization achievements.

Unsurprisingly, BIS is as unresponsive to the United States Congress today as it was then. BIS did not accomplish any of the GAO's recommendations. We should pause to ask ourselves where the U.S. would be today in the semiconductor arena had BIS attempted these recommendations. Likewise, we should ask where the U.S. will be twenty years from now, since BIS and their interagency partners have still not implemented controls for foundational technologies and only a few for emerging technologies that have since "emerged." The United States cannot afford to continue to rely on an unresponsive bureaucracy whose interests are not aligned with national security concerns and whose inaction is enabling the rise of America's most powerful adversary.

HUAWEI AND SMIC EXPOSE INEFFECTIVE U.S. EXPORT CONTROL POLICIES

Although the U.S. government instituted a set of export control reforms under the Export Control Reform Act of 2018, the rules still permit dangerous technology transfers to China. The CCP has proven itself to be masterful at sidestepping the boundaries of control and U.S. industry and export control officials have proven themselves to be adept at blindly accommodating that bad behavior.

The U.S. Government continues to approve transfers to Huawei despite a formal presumption of denial policy for the company: from November 2020 through April 2021, the USG approved 69 percent of transfer requests to Huawei.⁸ The primary reasons for such high rates of approval are due to U.S. export control officials changing review criteria from the standard presumption of denial policy to reviewing each transfer request separately with a much narrower focus to specifically restrict 5G technologies. As a consequence, a presumption of denial policy for Huawei only applies to technologies that facilitate 5G capabilities. Thus, all technologies unrelated to 5G are ripe for approval, an arguably foolhardy policy in light of the nascent competition to establish international 6G standards. Additionally, U.S. rules are written to allow Chinese companies to circumvent them easily. After the U.S. blacklisted Huawei in May 2019, for example, the company spun-off the smartphone company Honor to a state-owned company to maintain the flow of U.S. 5G technology.

Similarly, China's Semiconductor Manufacturing International Corporation (SMIC) is on the Entity List for its work with the PLA. The U.S. has a presumption of denial for transfers to SMIC, but only for technologies that are uniquely required for production of semiconductors at advanced technology nodes (10 nanometers and below, including extreme ultraviolet technology). Yet SMIC has recently introduced a 7-nanometer chip, is producing record revenues, and is on its way to becoming a behemoth in the global legacy chip market space. Yet the Department of Commerce approved or returned without action 99.5.% of all applications for SMIC from November 9th, 2020 to April 20th, 2021.⁹ It begs the question of whether continued U.S. exports to SMIC did not in some way unwittingly contribute to SMIC's 7-nanometer breakthrough, and thus better position the company to grab everbigger portions of the global chip market.

COMPLACENCY: WHY EXPORT CONTROL POLICY REMAINS BROKEN

From Alger Hiss in the 1950s, to Robert Hanssen in the 1980s and 1990s, to Jack Teixeira today, insider threats have always been a threat to American national security. But perhaps the most dangerous insider threat to U.S. military-technological supremacy comes not from a rogue leaker or spy, a naïve academician, an unsuspecting engineer with unprotected plans on his laptop, or a venture capitalist hungry for Chinese profits. The greatest insider threat is perhaps an arrogant complacency widespread among federal officials content with status quo export control policies.

While the U.S. government has in recent years expanded the Entity List and created a list of Military End Users (MEUs) that carry a presumption of denial for export licenses, in practical terms the policy does not produce as many automatic denials as intended. This adverse outcome has roots partly in the export license review process itself. Each export license application must be adjudicated on a case-by-base basis. Any denial of an export license must be substantiated with evidence, which costs much time and effort to obtain, to the extent it can even be produced. Because of limited intelligence visibility into China, the U.S. Government has little proof of actual diversion of technology to the PLA or MSS actually happening, and any known cases are just the tip of the iceberg. Much time is spent looking for needles in haystacks, and BIS places the onus on the denier to prove that the technology will be diverted (something that is nearly impossible to prove). All of these verification actions must take place within the 30-day statutory timeline for a license review, even as the number of China-related export license applications has increased in recent years. The cumbersome bureaucratic process and high burdens of proof to demonstrate Chinese malfeasence incentivize application reviewers to take the easier route of approving a license, which can be done in just a few clicks.

6 FLAWED RATIONALES FOR APPROVING CHINA-FOCUSED LICENSES

Many of those responsible for administering U.S. export control policies ignore national security concerns and rely on illogical justifications and false narratives to defend lax China-focused licensing decisions. Below are a few of the most common objections and the flaws inherent in them:

1. "There is foreign availability – if the U.S. does not sell the controlled technology to China, another country will." Consider the dynamics of one recently approved export control decision: Should the U.S. be willing to continue to assist in the repair of test equipment at a Chinese university that assists the PLA with nuclear weapons research just because a firm from some other nation might also supply such services? A desire to make sure U.S. firms prosper over foreign competitors may be a legitimate reason for approving a transfer that is not clearly destined for a military end-user. However, China's MCF policy means every transfer to China should still be viewed as a potential transfer to a military end-user. Additionally, many technologies of U.S. origin may offer unique capabilities in comparison to foreign varieties judged as mere equivalents. Why does China go to great lengths through its intelligence collection programs to obtain American technologies? Perhaps it's because the restricted U.S. technologies can supply unique capabilities that foreign alternatives cannot.

- 2. "It is low-level technology." Consistent with the logic above, if a technology would not provide a significant advantage to the PLA or MSS, a transfer of low-level technology would presumably not pose a national security risk. Such thinking does not, however, properly factor in why these technologies are controlled in the first place. Furthermore, the U.S. and other Western nations have often misperceived the military value of so-called "low-tech" dual-use exports from the U.S.
- 3. "The U.S. has set a precedent for supplying this technology to China." It is true that the U.S. has routinely shipped controlled items to China. But the security dynamic between the U.S. and China has changed in recent years. Decisions regarding past transfers were made in a different threat environment and should not govern future decisions. It would be counterproductive for the U.S. to continue to transfer dual-use technologies to China that could fuel military advancement, and in turn obligate DoD to spend scarce resources to develop countermeasures.
- 4. "Denying licenses would damage the U.S.-China trade relationship." With U.S. exports to China at \$151.1 billion in 2021, one could hypothesize that stopping the transfer of controlled technologies would have a dramatic impact on a trade relationship vital to both economies. Yet in 2021 the value of U.S. licensed-controlled exports to the PRC only constituted \$1.5 billion, only 1% of total U.S. exports to China.¹⁰ Denying the value of these exports entirely would hardly damage the overall U.S.-China trade relationship or the United States' 23 trillion-dollar economy.



- 5. "If we don't let them have useful technology, the Chinese will stop allowing genuinely large
 - *commercial sales.*" Many U.S. technology firms cite sales of cutting-edge controlled technology to China as the financing mechanism for their research and development activities. They declare that the new technologies that result from R&D work are in fact a larger source of overall revenue than the exports themselves. This deeply flawed logic essentially suggests that the U.S. continue to feed valued technology to China to enable the U.S. to maintain its technological edge over China. The reality is that this so-called edge continues to narrow. Earlier this year, the Australian Strategic Policy Institute commented that China has a "stunning lead" in research into 37 out of 44 critical and emerging technologies, including those with clear military uses such as artificial intelligence, advanced robotics, autonomous systems, and advanced aircraft engines (including hypersonics).¹¹ American technologies diverted, stolen, or legally transferred under rules governing joint ventures in China have no doubt helped create those advantages there is no reason to continue permitting their export to China.
- 6. "Restrictions and conditions on transfers to China mitigate the risk of diversion or proliferation." When U.S. officials impose end-use restrictions on technologies destined for China, they are

operating out of extreme naiveté in thinking they will be effective. Per the U.S.-China bilateral agreement on end-user checks, there is no viable means of verifying a product's final destination or use capabilities after 180 days following the transfer. A Chinese entity must merely pretend to be in compliance for that short period of time.

In a recent case involving the export of a large volume of sensitive microelectronic commodities, DOD approved the transfer on the condition that the Chinese end-user provide records and semiannual reports, and that the semiconductor devices produced must not have military end-use or military end-users, or applications for 5G, or space. In reality, these conditions are wholly nonsensical, as there is no way for the U.S. government to verify the records, reports, or ultimate stated end-use purposes. Any document from the Chinese Ministry of Commerce claiming that Chinese entities will honor a technology's end use is not worth the paper it is printed on.

U.S. END-USE CHECKS IN CHINA AND ENTITY LISTINGS DO NOTHING TO STOP CHINA FROM DIVERTING U.S. TECHNOLOGY TO THE PLA

U.S. end-use check policies inside China are practically useless, doing virtually nothing to mitigate the risk of diversion inside China, or prevent China from diverting technologies to countries such as Russia, Iran, or North Korea:

- The bilateral EUC agreement permits only <u>one</u> full-time Export Control Officer (ECO) to conduct pre-license checks (PLC) and post-shipment verifications (PSV) inside China.
- Chinese officials selectively permit or refuse this single officer to conduct export control checks, knowing that those companies where PSV are refused will be added to the Entity List.
- In other countries, U.S. export control officials can conduct post-shipment verifications with few
 restrictions for up to five years after a technology is shipped. But, unique to China, U.S. officials
 have only 180 days after an item is shipped to submit a request to conduct a check. After that China
 can do as it pleases with American technologies.
- The U.S. government conducts post-shipment verifications on only a tiny fraction of exports to China. I personally wrote a briefing memo for the Secretary of Defense using U.S. Commerce Department data highlighting that from 2016 to 2021, U.S. officials conducted on average only 55 end-user checks per year in mainland China. U.S government officials responsible for conducting these checks will attest to the extreme difficulty of accomplishing them.
- Reliance on the Entity List as a formidable tool to stop diversion is also very much misplaced. The U.S. government's reactive whack-a-mole approach to the Entity List fails to recognize the systemic nature of diversion under President Xi's MCF strategy. Business names, individuals, and addresses are easily and quickly changed, or new businesses established or transferred --as in the Honor case --to maintain the flow of needed U.S. technologies.

8 RECOMMENDATIONS FOR STRENGTHENING EXPORT CONTROLS TO DEFEND SENSTITIVE TECHNOLOGIES

In light of the numerous shortcomings noted above, a more predictable and responsible way to stop the PLA from obtaining American technologies is needed. Decades of internal executive branch attempts at policy or regulatory modifications have not fixed a broken export control system. The lack of success speaks to a need for timely congressional action to address the risks to national security. The following recommendations would arrest the hemorrhaging of U.S. militarily useful technology to the United States' greatest threat:

1. ELIMINATE THE GENERAL POLICY OF APPROVAL AND MAKE THE PRESUMPTION OF DENIAL POLICY THE DEFAULT POSITION FOR "NATIONAL SECURITY (NS)" CONTROLS TO THE PRC

Given that technologies controlled for national security reasons by definition, "make a significant contribution to the military potential," of a country,¹² all export applications for NS-controlled technologies destined for the PRC should carry a presumption of denial. Given that it is impossible to know actual end-use of any technology bound for China, the general policy of approval for civil end-use technology bound for the PRC according to EAR 742(7)(1) must end immediately.

2. ESTABLISH AND IMMEDIATELY ENACT A PRESUMPTION OF DENIAL POLICY FOR SPECIFIC CRITICAL TECHNOLOGIES DESTINED FOR THE PEOPLE'S REPUBLIC OF CHINA

In principle, predictability within an export control system is a prerequisite for industry to make sound business decisions and allocate resources. However, for the transfer of militarily useful technology to China, the predictable outcome should be one of denial, not approval. BIS's views of which technologies should be restricted are too narrow, and the Chinese Communist Party cannot be trusted to comply with U.S. end-use requirements. Establishing restrictive export controls and policies of denial would be the most effective tool for hindering China's military modernization goals and maintaining the edge of the U.S. warfighter. The U.S. must especially deny certain controlled and uncontrolled critical technologies, in particular where there is limited foreign availability:

- <u>Microelectronics</u>: For example, certain specific field programmable gate arrays (FPGAs), radiofrequency integrated circuits (RFICs) and monolithic microwave integrated circuits (MMICs) have many civil purposes. But they are also critical technologies used in some of the most advanced defense and aerospace platforms. China should not have the opportunity to obtain them.
- <u>Aerospace Technologies</u>: Gas-turbine engine technologies, such as hot-section technologies, FADEC systems, and composite materials represent some of the capabilities where there is limited foreign availability and are areas in which the U.S. has clear advantages. The U.S. has already fallen behind in hypersonics because of lax export controls. Congress needs to ensure that does not happen again in these areas.

• <u>Other Critical and Sensitive Technologies</u>: To help formulate additional technology-specific controls, Congress should invite the intelligence community to brief them on internationally-scarce critical and sensitive technologies on which the PRC depends.

3. GIVE THE DEPARTMENTS OF DEFENSE, STATE, AND ENERGY GREATER AUTHORITIES TO DETERMINE THE OUTCOMES OF LICENSE REVIEWS FOR CONTROLS WHERE THEY HAVE THE LARGEST EQUITY STAKE

BIS's track record of rubber-stamping export licenses and the irresponsibly high rates of approvals for the export of militarily useful technology to the PRC should prompt Congress to divest some of BIS's authorities to the other interagency stakeholders. These interagency stakeholders should have a greater ability to influence transfers for the various reasons for controls based on which Department has the larger equity. For instance, DOD should have a greater voice and ability to deny technologies controlled for national security and anti-terrorism controls. Since DOD will need to counter China's military capabilities in any potential future conflict with the PLA, it follows that DOD should have a greater ability to restrict technology transfers of any military consequence. The Department of State should be handed similar considerations for items related to regional stability and some of the multilateral non-proliferation regimes. Energy should have greater sway over nuclear technologies and the associated reasons for control.

Congress should likewise revamp the interagency process for resolving disagreement between federal agencies on export control decisions. The voting process for the Operation Committee, the body that adjudicates conflicts in licensing decisions (comprised of the Departments of Commerce, State, Energy, and Defense), should be updated so that a majority vote for a denial shall be the Operating Committee's final disposition, with no prospect for elevating the decision to ACEP. In the event of a two-to-two tie vote, the license should be denied. Elevation to the Advisory Committee on Export Policy, comprised of the same entities, should only be allowed in instances when agencies on the Operating Committee seek to overturn the approval of a license at the Operating Committee level.

4. REVISE TIMELINE REQUIREMENTS FOR TRANSFERS TO THE PRC

The federal government currently has 30 days to review transfer requests to China. This time period is inadequate. The federal government should be allotted additional time, e.g., 90, 180, or 365 days, to review proposed exports. The additional time will permit more meaningful analysis of potential military application, give the intelligence community more time to research potential end uses, and provide export control officers with additional time to conduct pre-license checks.

5. CONGRESS MUST DIRECT THE ADMINISTRATION TO RENEGOTIATE THE U.S.-CHINA END-USE CHECK AGREEMENT

The current agreement with China only permits U.S. export control officers to conduct verification checks up to 180 days after shipment, and only for technologies that meet certain criteria. The U.S. is also limited to one export control enforcement officer to cover all of mainland China. With every other trading partner, the U.S. can verify how all U.S. controlled technology is being used and who is using it for five to nine years following the transfer. The USG needs a new agreement with China that is consistent with international norms and provides for an increased number of export control

enforcement officers inside the PRC. Because we can expect the PRC to lie and withhold information at every turn, and given the official policy of MCF, absent a reliable mechanism to verify actual endusers and end-uses, the continued transfer of controlled technology to the PRC would demonstrate a continued willful blindness on the part of export control officials. While China is unlikely to agree to a renegotiation, it is worth trying to broker a new agreement if the alternative is denying all controlled technology.

6. AFFORD THE INTERAGENCY BODIES OVERSEEING EXPORT CONTROLS A GREATER ABILITY TO ESTABLISH CONTROLS FOR UNLICENSED AND EMERGING TECHNOLOGIES

Transfers of technology requiring a license are just a fraction of the total amount of militarily useful technology transferred to China every year. The total does not include the larger amount of exported U.S. technologies that flow to China with no license requirement, from EAR 99 commodities of perceived little technological significance to emerging and foundational technologies for which the U.S. has largely yet to establish controls, such as for additive manufacturing or quantum computing. These unlicensed transfers are also a significant resource for China's military modernization efforts. Congress should expand the authorities of the other export control stakeholders to add technologies to the Commerce Control List (CCL) if the reason for control falls primarily under their purview. These expanded authorities should provide key export control stakeholders, such as engineers at DOD who review technologies for potential military applications, a much clearer and quicker pathway for adding technologies to the CCL.

7. WORK WITH KEY PARTNERS AND ALLIES TO RESURRECT A MULTILATERAL EXPORT CONTROL REGIME SIMILAR TO THE FORMER COORDINATING COMMITTEE FOR MULTILATERAL EXPORT CONTROLS (COCOM)

The multilateral export control regimes are largely ineffective in implementing needed restrictions or adding additional meaningful controls in a timely manner. Three of the four main regimes are focused only on non-proliferation controls for weapons of mass destruction (WMD), and the Wassenaar Arrangement functions more as a transparency and coordination body for dual-use technologies than for proposing and implementing meaningful controls. Consequently, these regimes are ill equipped to adjust to the realities of the CCP's stated objectives of technological, economic, and military dominance.¹³

As the U.S. implements more consequential export control policies vis-a-vis the PRC, it should work with select like-minded international partners to establish technology specific controls among a few key players (similar to the semiconductor and SME controls) and establish multilateral export controls—a so-called Alliance of Techno-Democracies, as Martjin Rasser of the Center for a New American Security has described it.¹⁴ Participating states may wish to consider resurrecting the Coordinating Committee for Multilateral Export Controls (COCOM), multilateral body established shortly after World War II to restrict transfers of certain technologies to the Soviet Union and their satellite states, but dismantled in 1994.

Reviving a COCOM-like regime will permit partners to establish and harmonize more meaningful controls that the other multilateral regimes are not able to perpetuate. It will facilitate targeted

efforts in a multilateral setting to overcome the shortfalls associated with unilateral controls. It will expediate transfers of mutual benefit between member states. And it will help counter the CCP's malevolent plans of domination in key technology sectors.

Unfortunately, American credibility in marshalling a like-minded coalition is currently hindered by its status as one of the largest providers of controlled technology to China. In those instances where the United States has taken unilateral action, such as adding Huawei to the Entity List, its action provided leadership and top-cover for like-minded countries to follow.¹⁵ Congress can assume this mantle of global leadership by legislating much-needed change to the way the U.S. government controls militarily useful technology to the PRC. Such reforms will encourage partners and allies to establish similar China-related export control policies in a manner that works best for their particular system.

8. CONGRESS SHOULD ORDER A GAO AUDIT

BIS has a history of unilaterally disregarding Department of Defense conditions for licensing approvals, determining licenses are not required during reviews without consulting other stakeholders, and ignoring interagency requests and conditions for adding non-controlled or emerging technologies. Congress should order a Government Accountability Office (GAO) audit to access the extent of BIS disregard for regulatory authorities and access the risk to national security caused by violating established procedures.

CONCLUSION

The U.S. cannot afford to maintain its current export control policies toward China. U.S. industry, in collaboration with the U.S. government, is essentially underwriting China's military modernization. An immediate course correction to U.S. export control regulations and policies is required to ensure that U.S. technologies do not further facilitate China's military modernization efforts. The inability of the executive branch to effect change suggests that congressional action will be required. In turn, American regulatory and policy changes should form the basis for the U.S. to lead partners and allies to establish more meaningful controls and even form a new multilateral export control regime.

ENDNOTES

- 1 <u>https://www.bis.doc.gov/index.php/documents/</u> regulations-docs/2342-part-742-control-policy-ccl-basedcontrols/file
- 2 <u>https://www.wsj.com/articles/u-s-approves-nearly-all-tech-exports-to-china-data-shows-11660596886</u>
- 3 <u>https://www.wsj.com/articles/china-locks-information-on-the-country-inside-a-black-box-9c039928</u>
- 4 <u>https://www.washingtonpost.com/national-</u> security/2022/10/17/china-hypersonic-missiles-americantechnology/
- 5 <u>https://www.bis.doc.gov/index.php/documents/</u> <u>regulations-docs/2342-part-742-control-policy-ccl-based-</u> <u>controls/file</u>
- 6 <u>https://www.wsj.com/articles/u-s-approves-nearly-all-tech-exports-to-china-data-shows-11660596886</u>
- 7 https://www.gao.gov/assets/gao-02-620.pdf
- 8 <u>https://foreignaffairs.house.gov/wp-content/</u> uploads/2021/10/Huawei-Licensing-Information.pdf
- 9 <u>https://foreignaffairs.house.gov/wp-content/</u> <u>uploads/2021/10/SMIC-Licensing-Information.pdf</u>
- 10 <u>https://www.bis.doc.gov/index.php/documents/</u> <u>technology-evaluation/ote-data-portal/country-</u> <u>analysis/2971-2021-statistical-analysis-of-u-s-trade-with-</u> <u>china/file</u>
- 11 <u>https://www.reuters.com/technology/china-leads-us-global-competition-key-emerging-technology-study-says-2023-03-02/</u>
- 12 <u>https://www.bis.doc.gov/index.php/documents/</u> regulations-docs/2342-part-742-control-policy-ccl-basedcontrols/file
- 13 <u>https://cset.georgetown.edu/wp-content/uploads/</u> WorldECR-109-pp24-28-Article1-Wolf-Weinstein.pdf
- 14 <u>https://www.cnas.org/publications/commentary/the-</u> case-for-an-alliance-of-techno-democracies
- 15 <u>https://www.uscc.gov/sites/default/files/2022-04/Nazak_Nikakhtar_Testimony.pdf</u>

WILLFUL BLINDNESS

AN INSIDER'S ACCOUNT OF HOW AMERICA'S INEFFECTIVE EXPORT CONTROL REGIME INCREASES CHINESE MILITARY STRENGTH

BY STEPHEN COONEN, CHINA TECH THREAT SPECIAL ADVISOR



www.chinatechthreat.com