Arms Control and International Security Papers
Volume I | Number 8
May 22, 2020

U.S. National Security Export Controls and Huawei: The Strategic Context in Three Framings

by Christopher A. Ford

The Arms Control and International Security Papers are produced by the Office of the Under Secretary of State for Arms Control and International Security in order to make U.S. State Department policy analysis available in an electronically-accessible format compatible with "social distancing" during the COVID-19 crisis.

Volume I, Number 8 | May 22, 2020

U.S. National Security Export Controls and Huawei: The Strategic Context in Three Framings

by Christopher A. Ford[1]

In this latest addition to the *ACIS Papers*, Assistant Secretary Ford discusses recent U.S. moves to restrict transfers of cutting-edge U.S. technology to the Chinese technology company Huawei, explaining these steps and placing them in the strategic context of a great power competition with the People's Republic of China (PRC) brought on by Beijing's geopolitical revisionism, exploitation of such firms to steal and divert foreign technology to support the Chinese military, abuses of human rights in China itself, and employment of companies such as Huawei as tools of strategic influence.

The United States, along with its Allies and partners, are today in the midst of an extremely important shift of approach when it comes to national security export control policy vis-à-vis the People's Republic of China (PRC) – including with respect to the Chinese technology company Huawei, the world's largest telecommunications equipment manufacturer. Under the Trump Administration, the United States has made some very significant changes to our export control policies and regulations, but it is important not merely for the policy community to understand these changes in themselves, but also for everyone to understand the *reasons* for them and the *strategic context* in which these adjustments are embedded.

Accordingly, this latest in the State Department's *ACIS Papers* series attempts to provide the background for three major tranches of Huawei-related changes: (a) the placement of Huawei on the Commerce Department's "Entity List" in August 2019; (b) the adjustments the United States announced in April 2020 to the "military end-use/user" (MEU) regulations and the "CIV" and "APR" license exception categories; and, most recently, (c) changes to the Foreign Direct Product Rule (FDPR) with regard to the export or use of high-technology semiconductor equipment and design tools. This *ACIS Paper* will thus situate these adjustments in the full context in which they need to be understood – specifically, as part of an ongoing U.S. effort to respond to the challenges that have unfortunately been created by the PRC's manipulation and exploitation of China-based entities (and Chinese citizens) in support of the Chinese Communist Party's (CCP's) efforts to remain in power in the PRC and to seize for itself the commanding heights of military and technological power in the mid-21st-Century geopolitical arena.

I. Three Perspectives on the Huawei Policy "Landscape"

To help elucidate the context in which the "Huawei problem" is embedded, and which has necessitated these

[1] *Dr. Ford serves as U.S. Assistant Secretary of State for International Security and Nonproliferation, and is additionally performing the Duties of the Under Secretary for Arms Control and International Security. He previously served as Special Assistant to the President and Senior Director for Weapons of Mass Destruction and Counterproliferation on the U.S. National Security Council staff.*

export control changes, this paper will look at that problem from multiple angles. Huawei is a PRC-state-supported information and communications technology firm that serves as a tool of manipulation and influence for the CCP, both at home and abroad, and of course the company is therefore nothing whatsoever like a beautiful ancient Chinese painting. Nevertheless, I hope the reader will forgive a loose analogy to Chinese art as we look at the challenges Huawei presents to the United States and to many other countries around the world.

It is not uncommon in Chinese landscape painting – as seen, for instance, in the early 11th-Century masterpiece *Travelers among Mountains and Streams* by Fan Kuan, a classic of Northern Song landscape painting that is currently in the permanent collection of the National Palace Museum in Taiwan – for an artist to employ multiple different perspectives in the same painting. This ancient approach made no use of the "laws" of one-point linear perspective later articulated in the Italian Renaissance during the 14th and 15th Centuries. Instead, works such as Fan's *Travelers* often painted the foreground, middle ground, and distance as if each were being seen from a slightly different angle, *yet at the same time*. This was not so much a technical failing, one presumes, than it was simply a way to help the viewer appreciate a landscape more fully – albeit less "realistically" – than is arguably possible with merely a single, quasi-photographic perspective. Such overlapping perspectival framing permitted immediate visual access to more facets of a scene than could be directly apprehended from a single vantage point.

Taking that artistic insight as inspiration, therefore, this paper will offer three overlapping and complementary perspectives upon the Huawei challenge that the Western world faces today, and upon what we in the U.S. Government are doing to meet it. Each of these framings is valid, significant, and compelling in its own right, but the reader will benefit most – and be able more fully to appreciate the U.S. position – by having all three of these overlapping and complementary perspectives spelled out distinctly.

A. Technology Theft

The first of these perspectives has to do with theft – specifically, the theft of cutting-edge U.S. technology by the PRC acting through its instrumentality Huawei. In this respect, the Huawei export control saga began in January 2019, with the indictment of Huawei and one of its affiliates by the U.S. Department of Justice for a range of crimes – specifically, bank fraud and conspiracy to commit bank fraud, wire fraud and conspiracy to commit wire fraud, violations of the International Emergency Economic Powers Act (IEEPA) and conspiracy to violate IEEPA, and conspiracy to commit money laundering. In short, as one U.S. Attorney described the situation, the indictment charged that "[f]or over a decade, Huawei employed a strategy of lies and deceit to conduct and grow its business."

Thus surfaced the first wave of concerns over Huawei's alleged role in stealing U.S. technology for its CCP masters.[2] In the wake of this indictment, the State Department's Bureau of International Security and Nonproliferation nominated Huawei to be added to the Commerce Department's "Entity List" of foreign actors that are understood to be involved in potential diversion of items to weapons of mass destruction programs or in "activities contrary to U.S. national security and/or foreign policy interests." In May 2019, the company and 68 of its non-U.S. affiliates were added to the Entity List. An additional 46 foreign affiliates of Huawei were added in August 2019.

Since then, this problem of outright theft and illegality has only become worse. In February 2020, the Department of Justice – after having investigated further – filed a superseding indictment, further charging Huawei and several of its subsidiaries with conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (RICO), through "decades-long efforts," in the United States and in the PRC, involving

> "[the] misappropriat[ion] [of] intellectual property, including from six U.S. technology companies, in an effort to grow and operate Huawei's business. The misappropriated intellectual property included trade

[2] For present purposes, I shall leave aside the aspect of the Huawei case that related to Iran policy, but readers should remember that the IEEPA violations with which Huawei was first charged related to the company's alleged role in assisting Iran in evading U.S. sanctions. This was, therefore, yet another layer of our concerns about Huawei, for we obviously could not stand by while a PRC company helped the clerical regime in Tehran earn more of the revenue it needs to expand its nuclear capabilities, develop and proliferate missiles, undertake expeditionary warfare against its neighbors using Qods Force subversives, and support terrorist networks in the Middle East and farther afield.

> secret information and copyrighted works, such as source code and user manuals for internet routers, antenna technology[,] and robot testing technology."

The proceeds from this racketeering activity, the indictment alleged, were reinvested in Huawei's worldwide business, including in the United States.[3]

To be sure, Huawei's involvement in such theft hardly makes it a unique case in the Chinese high-technology sector. Unfortunately, just this sort of intellectual property theft by PRC entities is routine and rampant. But these indictments *did* make a compelling case that we needed to approach such thieves differently from an export control perspective. Just as with the PRC's China General Nuclear Power Company (CGNPC) – which was indicted in April 2016, along with one of its employees in the United States, for illegally trying to obtain U.S. technology for Chinese nuclear reactor programs, and whose activities in not just stealing U.S. nuclear reactor technology but also in diverting it to the PRC's armed forces led us to revise our civil-nuclear export control rules for the PRC – Huawei's indictment for similar thievery made clear that we could not continue export control "business as usual" with it.

This, then, is one important perspectival framing of the Huawei problem. The PRC, of course, is notorious for not respecting the rule of law, as well as for its opaque, closed, corrupt, and unaccountable system of governance. Indeed, the PRC weaponizes Western legal scrupulousness and commitment to a free and open international order to gain competitive advantage. Its leaders have been effectively immune from law enforcement scrutiny and action, and at arms length from the ordinary consequences that should flow from impartial audits and the accountability of democratic governance. In the CCP's playbook, rules are things to which *others* should be held accountable when this proves useful to the success of the PRC's domestic industry champions and the accretion of the PRC's power globally. When it comes to restrictions *against* Beijing, however, the CCP regime seems ever less interested in accountability as the PRC's power grows.

Does the PRC respect the Universal Declaration of Human Rights? Not when the CCP wishes to undertake a campaign of repression against its own citizens, including against members of ethnic and religious minority groups in Xinjiang, where more than one million individuals have been detained in internment camps since April 2017. Does Beijing respect the findings of the international tribunals adjudicating maritime claims in the South China Sea? Not so long as it wants to seize that area for itself and violate Xi Jinping's own prior promises by building a constellation of military bases on tiny man-made islands. We in the United States take very seriously the obligation under Article VI of the Nuclear Nonproliferation Treaty (NPT) to pursue negotiations in good faith on effective measures to end the arms race, but what does Beijing think? In December 2019, we formally invited the PRC in good faith to begin a strategic security dialogue on nuclear risk reduction, arms control, and their future – but at the time of writing, many months later, we still await Beijing's response.

Does the PRC even respect the CCP regime's *own* longstanding arguments about the importance of "non-interference" in the "internal affairs" of other states? Not when it wants to bully other countries about how they describe the PRC *in their own domestic media* or when it objects on political grounds even to street art thousands of miles away in another sovereign state, or when the CCP wants to threaten a foreign government in order to stifle international calls to investigate how the terrible COVID-19 virus was able to spread so far so quickly while PRC authorities suppressed warnings by doctors in Wuhan.

In such cases, where the PRC sees a chance to seize advantage over others, transparency, accountability, and the rule of law are of little interest to the CCP regime, and indeed may even be considered threatening to it. Fundamentally, the PRC's system of governance is grounded not in the rule *of* law but rather in the Communist Party's rule *by and through* law, for the Chinese Communist Party itself is conceptually and structurally antecedent to the PRC's legal system, the purpose of which is to serve the party. (With apologies to Voltaire, who once made a similar point about the relationship between 18th Century Prussia and its army, it might be said that while many states have political parties, in the PRC the Communist Party has its own *state*.)

This attitude toward law goes back a long way. In their propaganda narratives, PRC officials like to emphasize themes deriving from China's Confucian heritage, with its emphasis upon benevolence and virtue in leadership. In

[3] The second U.S. indictment also included new allegations about the involvement of Huawei and its subsidiaries in business and technology projects in countries subject to U.S., European Union, or United Nations sanctions, such as Iran and North Korea, as well as about its efforts to conceal these efforts to help such rogue regimes.

reality, however, the governing philosophy of the CCP owes more to ancient Chinese Legalism, a philosophy that aimed at achieving and consolidating absolute power, and which saw the purpose of law as being to support the power of the ruler rather than to make power in any way accountable. Such Legalist advice from the scholar Shan Yang in the 4th Century B.C.E., it is recorded, helped Duke Xiao begin positioning the state of Qin for its long march of conquest over all the other polities of China's ancient Warring States period, which eventually unified the country and created the notoriously tyrannical (if short-lived) Qin Dynasty in 221 B.C.E. from which "China" gets its name. In some respects, unfortunately, it would appear that not too much has changed today.

In the modern technology-transfer context, the results of the PRC's self-aggrandizing and selectively scofflaw attitude have been all but catastrophic for the rest of the world. Illegal, often cyber-facilitated intellectual property theft by PRC entities has helped lead to what former U.S. National Security Agency director Keith Alexander has described as "the greatest transfer of wealth in history."

The crimes for which Huawei has been indicted, therefore, may only be one piece of a broader PRC technology-theft problem, but they are an important part – in connection with which it was necessary for the United States to take a principled stand. I'm proud of the role my Bureau played in nominating Huawei for the Entity List, for U.S. exporters indeed *should* think twice before engaging with foreign companies that steal U.S. technology – especially when they are doing so as part of a broader pattern of state-organized theft.

B. Strategic Competition Perspective

But mere technology theft, *per* se, is only one part of the Huawei problem. The challenge – indeed the threat – presented by the PRC and its *de facto* instrumentalities such as Huawei is much greater than that. The relevant context here is the PRC's drive to seize a dominant share of global high technology markets as quickly as possible, such as under its infamous "Made in China 2025" strategy. Crucially, these efforts are *not* being made simply for profit and to drive foreign competitors out of business, but also in support of the PRC's geopolitical ambitions of a so-called national "return" to the dominant center of the geopolitical system.

This PRC strategy represents, almost by definition, a mortal threat to non-Chinese technology sectors, even if not all of them yet realize it, with some Western firms still transfixed even today by the short-term profits available from selling to PRC entities even while their Chinese competitors gather strength from non-competitive and illegal actions and PRC state subsidies, intending eventually to supplant such Western suppliers everywhere. That certainly is, in itself, a huge problem. But all of this – as we have emphasized repeatedly – is also a *global security* threat, as a result of the embeddedness of the PRC's technology-transfer strategy in the CCP's aggressively competitive geopolitics of hegemony in East Asia and more broadly.

PRC theorists believe that technology and economic weight contribute, along with military muscle, to something called "comprehensive national power" (CNP), which is in effect a modernized and Sinicized version of what Soviet geopolitical theorists used to refer to as the "correlation of forces" that they felt would eventually allow their Marxist empire to overcome the capitalist West in *that* era's geopolitical competition. The ultimate purpose of Beijing's strategy thus isn't simply economic advantage, market share, and corporate profits – though in contrast to the USSR, today's state-capitalist PRC both seeks and enjoys those things – but also geopolitical and strategic advantage. Building superlative CNP is viewed as the key to acquiring dominant global power, something that others enjoyed vis-à-vis Beijing in the past, and which the CCP now intends to acquire for the PRC. This is Xi Jinping's "China Dream," and acquiring controlling positions across a critical range of cutting-edge technologies is a critical part of the PRC's revisionist geopolitics.

It is for this reason that we have tirelessly warned about the dangers presented by the PRC's strategy of "military-civil fusion" (MCF). With CNP seen as the key to acquiring global power, implementation of MCF is, in Beijing's view, the key to the PRC developing the most advanced military in the world by 2049 – which is expected to provide the CCP regime with a commanding position in global "hard power." In pursuit of such next-generation military dominance, MCF aims, to break down all barriers between the civilian sector and the military sector in the PRC, and to marshal the resources and know-how of both spheres – through coercion if necessary – in support of the CCP's revisionist agenda. I have been publicly warning about the dangers of MCF since July 2018, and buoyed by Secretary Pompeo's powerful articulation of these challenges in a pathbreaking recent speech in Silicon

Valley, we have been gradually reorienting the U.S. foreign policy and national security apparatus around the challenges of meeting this threat.

Make no mistake: Huawei is a major player in this PRC strategy. The company, for instance, sells its "Unified Communications and Collaboration" technology to several elements of the People's Liberation Army (PLA) and the PRC security services, including the PLA's General Staff Department, the Beijing Military Region, the 2nd Artillery Corps (now the PLA Rocket Forces), and the Ministry of State Security (MSS). Huawei also has strategic cooperation relationships with state-owned enterprises involved with military production, including the China Shipbuilding Industry Corporation's 719 Research Institute, which has been involved in the design of nuclear submarines and sea-based nuclear power plants. Huawei employees have, moreover, worked closely with PLA institutions, and in some cases appear actually to be "dual-hatted" as employees of state-owned defense enterprises. And Huawei's 5G telecommunications capabilities make it a key player in supporting the PLA's drive for dominance in what PRC strategists term "6th Generation" or "intelligent warfare," which they expect will depend upon Artificial Intelligence (AI) capabilities riding on a 5G backbone.

So this, then, is the context for my second "perspective" on the Huawei problem. The PRC's MCF strategy has required a rethinking of how to approach national security export controls, because the CCP's approach to acquiring foreign technology and diverting it to the PRC's military and security services makes rather a hash of traditional approaches to export controls, which tend to presume a meaningful distinction between "civilian" and "military" that is becoming increasingly opaque, or even meaningless, in the PRC. Driven by such concerns, we have begun making adjustments to U.S. export control regulations, such as – as will be outlined hereinafter – in the definition of what can count as a "military end-user" and in the elimination of the so-called "CIV" category of export license exception vis-à-vis the PRC.

C. Human Rights Perspective

In my view, each of the first two perspectives I have offered here upon the Huawei problem are on their own enormously compelling. Nevertheless, there is a *third* way to frame the policy problem presented by Huawei – along with many of its siblings in the state-supported Chinese high-technology sector – that provides further reasons for any democratic government to shun such companies.

As I pointed out in September 2019, across the malignant ecosystem of the PRC's technologized authoritarianism, there is constant and continual cooperation between companies such as Huawei and the state security bureaucracy. Nor is such cooperation optional for these companies if, when, and to the degree that the CCP commands such cooperation. And it is here that Huawei's various partnerships with the PLA, the MSS, and various military research institutes within PRC state-owned enterprises become even more sinister.

The Wujiang Public Security police, for instance, use Huawei technology to impose CCP controls upon the PRC's citizenry, and Huawei's own documents brag about providing the security police with high-technology "social stability" solutions in Pingan. If you have any familiarity at all with the police state that the CCP has built, of course, you'll know that this is nothing at all to brag about, but the role of PRC technology giants such as Huawei in enforcing and supporting CCP tyranny is well established on the public record.

Despite its pretensions to philosophical depth and world-historical themes of pseudo-Marxist dialectical progression and benevolent quasi-Confucian meritocracy, the Chinese Communist Party's most original and significant contribution to human governance lies in its pioneering of a technologically-facilitated form of totalitarianism the likes of which humanity has never seen before. Tragically, Huawei and its siblings have distinguished themselves as enablers for and handmaidens of this new form of oppression. What's more, they are making their technology – and thus the CCP's repressive model – *available for export*, by offering surveillance tools and methodologies, in the name of "smart cities" and "safe cities" technologies, among other more readily obvious tools of suppression, to foreign governments, some of which are eager to replicate for themselves the iron grip that the CCP exercises upon the Chinese people.

In the context of our relationship with Huawei, therefore, this is yet another reason why export control "business as usual" is impossible, and why it is a moral imperative for the democracies of the world to avoid entanglements with the CCP's high-technology authoritarianism. In the United States, we want our companies and citizens to avoid making such abuses profitable, and to avoid helping reward such egregious

conduct through commercial profits. To my eye, no one who takes human rights seriously would want to do anything *other than* shun PRC companies such as Huawei.

Together, therefore, these three perspectives on the "landscape" of Huawei-related policy issues[4] should help explain the United States' new approach to export controls vis-à-vis that company – and why such a new path has turned out to be so necessary. The next section of this paper will briefly describe our responses to these threats to date, in putting Huawei on the "Entity List," adjusting certain U.S. export control rules in light of the PRC's MCF strategy, and making Huawei-related changes to the Foreign Direct Product Rule (FDPR).

II. Our Responses

A. The Entity List

As noted earlier, we put Huawei on the Commerce Department's "Entity List" in May 2019; we also added additional Huawei affiliates to the list in August 2019. This was an essential predicate for properly evaluating and responding to the Huawei problem, inasmuch as most U.S. exports to Huawei did not previously require an export license. By placing the company on the Entity List, we required licenses (with a few minor carveouts related, *inter alia*, to keeping telecommunications infrastructures and personal communications devices operational) for *all* transfers to Huawei, giving us visibility – for the first time – into the items and technologies it was acquiring from U.S. industry.

Although that listing came with a presumption of denial, this did not necessarily mean that we necessarily intend to deny all such transfers. Being placed on the Entity List triggers a licensing requirement, but it does not in itself decide the outcome that results from evaluating such licenses. Naturally, in light of what we now know about Huawei – and what we unfortunately continue to learn as time goes by – we are looking at such licenses with an increasingly skeptical eye that generally presumes rejection,[5] but "listing," *per se*, does not equate to "denial." It merely means that the U.S. Government deems it important to *evaluate* such questions, and this represents an important step forward for transparency and accountability in technology transfers. With regard to Huawei, this was our first step.

B. Export Regulation Adjustments

The second major adjustment in U.S. rules vis-à-vis Huawei became clear in late April 2020, when the Department of Commerce announced an expansion of controls to "military end-users" (MEUs) in China, which include commercial entities when their functions are intended to support defined "military-end uses." Commerce also expanded the list of Export Control Classification Numbers (ECCNs) subject to MEU licensing requirements in light, *inter alia*, of past diversions of controlled items for military purposes and end-users that did not require a license for export. These changes were necessary in response to the PRC's MCF strategy – which, as noted above, has been systematically eroding prior distinctions between what is "civilian" and what is "military" in China.

These changes were hardly what we really *wished* to do, and we would have preferred to continue prior policies of exporting more liberally to "civilian" applications in the PRC. MCF, however, has made that idea incoherent, for *in effect, there is no longer any such thing as a purely "civilian" export to the PRC*. This certainly doesn't mean that we intend to deny all covered exports to the PRC, but the CCP regime's work to "fuse" the PRC's civilian and defense

[4] In truth, there is yet another potential perspective upon the Huawei problem that is worth mentioning here, related to the ways in which – under well-established PRC law and the extraordinary tools available to the CCP in coercing whatever behavior it wishes from Chinese citizens and companies operating either at home or abroad – the CCP is able to compel companies such as Huawei to do its bidding whenever it wishes. In this context, and in sharp contrast with Western firms' relationships with their own governments, it is important to remember that, at least in particular instances in which the CCP cares to make its will known, *there is, functionally speaking, no distinction between "private" PRC companies and the government*. Accordingly, Huawei must be regarded as a tool of strategic influence by the CCP regime in Beijing, and permitting oneself to become dependent upon a company such as Huawei for such things as one's 5G telecommunications infrastructure is the same thing as giving the CCP the option of exerting direct control over that infrastructure – to manipulate it, or to deprive you of its functionality for purposes of political extortion, howsoever the CCP desires. Nevertheless, since such potential strategic manipulation is not directly relevant from the perspective of U.S. export controls, I will not dwell upon it further here.

[5] By way of full disclosure, while the Commerce Department administers the broader U.S. export control system, the Bureau of International Security and Nonproliferation screens U.S. export control licenses for nonproliferation and other technology-transfer implications.

industrial bases in support of regional hegemony and global revisionism has made it impossible for us to continue to permit exports without a greater degree of scrutiny. Irrespective of what licenses we *deny*, therefore, it is vital for U.S. authorities to be able to see, and to assess, what items and technologies are being transferred into the CCP's MCF apparatus.

This is also the rationale behind the United States' accompanying elimination of the "Civil End User" – or "CIV" – category of license exception vis-à-vis the PRC. It is also the basis for our proposal to eliminate certain "Additional Permissive Reexport" (APR) license exception permissions that previously allowed partner countries the ability to re-export U.S.-origin controlled items to countries such as the PRC without an export license from the Department of Commerce. As that Department outlined its public explanation of the proposed APR change, it is considering this move because other countries might take differing views of what it is appropriate to send to the PRC. Not surprisingly, we do not wish our own technology protection policies to be undermined through incautious re-export transfers to the PRC by those who do not yet share our perspective on the importance of principled resistance to Beijing's theft of technology and its diversion to military purposes, its human rights abuses, and its geopolitical revisionism. Our hope is that this proposed rule will give partners an opportunity to join our efforts. Either way, however, only the CCP itself is to blame for these actions.

C. The Foreign Direct Product Rule

The most recent of our export control changes vis-à-vis Huawei is the announcement of revisions to the FDPR in order to restrict Huawei's ability to circumvent U.S. export controls by designing semiconductors and having them produced abroad using U.S. software-based design tools or equipment. With these FDPR adjustments, the United States is imposing licensing requirements on these foreign-produced items when there is knowledge that they are destined for Huawei (or for affiliates appearing on the Entity List). As a result, foreign items – including chipsets – that are produced *anywhere* from the designs of Huawei using U.S. Department of Commerce-controlled semiconductor manufacturing equipment or software will be subject to U.S. export licensing restrictions when there is knowledge they are destined for Huawei or one of its listed affiliates.

This is a very significant move, since while many sorts of semiconductor technology are by now widely available on global commercial markets from many suppliers, U.S. firms still enjoy a significant competitive advantage on many of the very best tools for designing and producing high-end semiconductors (*e.g.*, chips with "nodes" of extremely small size, which permit enormous amounts of computing power to be crammed into a tiny physical space). The PRC also targets advanced technology from a small number of like-minded countries such as Japan, the UK, the Netherlands, and Germany, but the United States maintains the lion's share of technological advantage. The PRC has hitherto procured top-notch chips from the United States and a few like-minded countries, and it is of course seeking to acquire such high-end manufacturing capabilities for itself, but at present this represents an arena in which the United States and our partners maintain a huge competitive advantage. The new rule will constrain Huawei's ability to design the very best chips, as well as its ability to access to the superlative manufacturing tools still provided by U.S. suppliers, to produce them.

This new FDPR is designed to minimize its adverse impact upon U.S. (and other Western) suppliers. Indeed, this move may serve to help U.S. firms maintain their dominant market position in the very upper reaches of the semiconductor design and manufacturing business, by restricting Huawei's access to the "secret sauce" ingredients that produce the world-class chips and high-end design tools that are today still available exclusively from U.S. industry. More fundamentally, these adjustments should help impede the progress of Beijing's MCF apparatus as it seeks to appropriate and redirect cutting-edge Western technology to support the CCP's dreams of geopolitical revisionism.

III. Conclusion

These are not challenges that we sought. Quite to the contrary: none of these changes in U.S. export control policy in response to PRC technology-transfer, human rights, and geopolitical challenges are ones that we *wished* to make. Confronted with the realities of Beijing's ambitions and the PRC's "military-civil fusion" strategy, however, we had little choice but to act decisively.

The United States has long been committed to open and free trade for mutual benefit with the PRC, and it must always be remembered that – as my colleague, Assistant Secretary David Stilwell, powerfully recounted last year – it was actually the United States' *embrace* of the PRC over most of the last generation that has been perhaps *the* critical component in the PRC's modern rise to geopolitical

prominence. Nevertheless, the Chinese Communist Party's flagrant abuse of all this American and global goodwill for its own hegemonic self-aggrandizement has been nothing less than shocking, and the world is now awakening to that fact. And we must respond accordingly.

Today, U.S. policy seeks to navigate between unpalatable extremes. When it comes to the PRC, we are not nearly as naïve as we used to be about the potential for unrestricted foreign economic and technological engagement to feed the CCP's military ambitions and geopolitical self-aggrandizement at the expense of our interests, and at a grave cost to the freedom and autonomy of the PRC's own neighbors. Our hope is to bring our close partners to this realization as well, and we are pleased by the progress we are making so far.

We are today not, for instance, open-heartedly foolish in the ways suggested in Thucydides' rendering of Pericles' famous funeral oration for Athens' early casualties in Peloponnesian War:

> "We throw open our city to the world, and never by alien acts exclude foreigners from any opportunity of learning or observing, although the eyes of an enemy may occasionally profit by our liberality …."

Nor, however, are we needlessly paranoid and restrictive about engaging with foreigners in the high-end technologies of our day – as were, for example, the Venetian officials who in 1745 actually dispatched an assassination team to pursue two local glass-blowers who had taken the lucrative secrets of their trade abroad.[6] In truth, the right answer surely lies between such asymptotes, and – as in so many other arenas – we will all suffer if we cannot navigate a prudent middle way between such extremes. In the arena of national security export controls, it is just such an Aristotelian Mean of a response that we have been trying to implement.

The United States' new export control rules are intended to be effective answers to the challenges so far presented by PRC firms such as Huawei, but yet responses that still preserve the possibility of beneficial engagement with the PRC. It continues to be our view that the Sino-American relationship needs to be cooperative where it can be, even as we are now demonstrably committed to ensuring that this relationship is appropriately *competitive* where the CCP regime leaves us no choice but to be so. The most recent adjustments to the FDPR, for instance, must be seen in this light, and in the broader context of the challenges that PRC revisionism and disrespect for international norms and the rule of law have forced upon the world. We look forward to the day when it is no longer necessary to respond to such threats from the Chinese Communist Party.

* * *

[6] *See*, e.g., Christopher Andrew, *The Secret World: A History of Intelligence* (New Haven: Yale University Press, 2018), at 33 & 131 footnote.

Volume I, Number 8 | May 22, 2020

Arms Control and International Security Papers

The Arms Control and International Security Papers are produced by the Office of the Under Secretary of State for Arms Control and International Security in order to make U.S. State Department policy analysis available in an electronically-accessible format compatible with "social distancing" during the COVID-19 crisis.