Arms Control and International Security Papers
Volume I | Number 23
December 7, 2020

Technology-Transfer De-risking: A New and Growing Need

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 23 | December 7, 2020

Technology-Transfer De-risking: A New and Growing Need

by Christopher A. Ford[1]

In this ACIS Paper, Assistant Secretary Ford explores the emerging issue of "de-risking" as applied to engagements with the technology sector of the People's Republic of China (PRC), stressing the need for commercial actors to ensure that technology-related engagements with China are not abused, and describing the emerging arena of "technology transfer de-risking" (T2D), which is of increasing importance for commercial entities and financial institutions that wish to avoid reputational risk, to prevent potential future U.S. sanctions or penalties, and to keep their involvement with the PRC from inadvertently supporting human rights abuses and fueling destabilizing military developments.

This paper looks at the phenomenon of "technology transfer de-risking" (T2D) in the context of longstanding and ongoing efforts by the People's Republic of China (PRC) to blur – and ultimately, Chinese Communist Party (CCP) leaders hope, entirely to erase – any distinction between the country's "civilian" and "military" industrial bases and technology sectors. It argues that both government and civilian entities in the democratic world, and particularly commercial and financial institutions of the private sector, should pay more systematic and prudential attention to elements of risk associated with economic and especially high-technology entanglement with the PRC, making T2D increasingly into a routine element of business practice.

I. What is De-Risking?

Before addressing these questions, however, it is useful to recount what we mean by "de-risking," a term used in various contexts, with different degrees of clarity, and belonging to a spectrum of responses that commercial and financial actors employ when faced with risks. Accordingly, we should be careful to be clear here.

"De-risking" is arguably best known in the context of anti-money-laundering (AML) compliance, but the concept is a significantly broader one. Across the different fields in which the term is used, it denotes the avoidance of a risk through avoidance of the activity that entails the risk. In one of the main fields where the term is used, financial

[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.*

services, as explained by the Financial Action Task Force, "de-risking"

> "refers to the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk …. De-risking can be the result of various drivers, such as concerns about profitability, prudential requirements, anxiety after the global financial crisis, and reputational risk. It is a misconception to characterise de-risking exclusively as an anti-money laundering issue."

Of course, it does not make sense to obligate terminating, or even restricting, every activity that carries a risk. For that matter, it does not make sense for policymakers even to nudge financial and commercial actors toward a de-risking approach where no vital policy goal is involved or where de-risking is not the best way to pursue such a goal. Careful assessment of benefits and risks are necessary here. Some activities, though carrying risk, are best continued with risk mitigation measures in place as safeguards, rather than being curtailed altogether.

But with respect to certain activities in certain areas where certain actors are involved, the risks weigh more heavily toward restriction and even avoidance. Thus, though we do not wish to see important goods and services withheld from whole countries or communities under an indiscriminate de-risking approach, de-risking should never be off the table altogether. With the increased emphasis the international community has placed upon nonproliferation in the last two decades, *nonproliferation* de-risking has emerged as a growing area. Numerous U.N. Security Council resolutions (UNSCRs) adopted pursuant to Chapter VII of the United Nations Charter, for instance, now require all UN Member States to impose sweeping sanctions against North Korea on account of its weapons of mass destruction (WMD) programs, and broad nuclear-related sanctions against Iran have also now come back into force pursuant to the terms of UNSCR 2231 (2015). Additionally, UNSCR 1540 has since 2004 required all UN Member States to refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer, or use nuclear, chemical or biological weapons, or their means of delivery. In short, de-risking over the past two decades has joined the nonproliferation toolkit.

As both international rules and an expanding corpus of domestic law have grown up in this area – augmented by robust efforts by U.S. authorities to respond to sanctions evasion – it is increasingly common for financial and commercial due diligence to include attention to nonproliferation equities, for reasons not merely of legal risk but also of reputational harm.

But "de-risking" policies and practices are not limited solely to violations of U.S. nonproliferation sanctions, where heavy penalties lie in wait for those who do not do enough to avoid facilitating abuses by their clients and customers. Attention is also increasingly being paid to de-risking where the potential for direct harm to private sector actors is largely reputational, such as where specific activities or commodities are likely to implicate them in unsavory things such as labor abuses and human rights abuses committed by their commercial counterparties overseas.

"De-risking," then can be seen as part of a spectrum of available responses through which commercial and financial actors take prudential steps to partially or wholly protect themselves and their investors against various types of harm that can inadvertently result from the policy externalities – *e.g.*, facilitating international drug trafficking, WMD proliferation, or human rights abuses – created by incautious business decisions. It is the thesis of this paper that such due diligence thinking should also be extended to involvement with PRC counterparties involved in problematic activity, with particular attention to the risks of technology diversion to military applications.

II. Risks and Challenges of Sensitive Transactions with the PRC

A. General Problems

It is no secret, of course, that commercial dealings with and investments in the PRC entail special challenges and risks. U.S. financial regulators, for instance, have warned that corporate stock offerings, financial prospectuses, and other instruments coming out of China involve "substantially greater risk that disclosures will be incomplete or misleading and, in the event of investor

harm, [there will be] substantially less access to recourse." PRC environmental and labor standards are notoriously poor, even high-profile sectors such as nuclear reactor safety regulation take shortcuts in the name of sectoral expansion in order to meet government expansion targets, and intellectual property theft from foreign commercial counterparties has been routinized – even where sweeping technology transfers were already required under PRC law – pursuant to government policies explicitly devoted to helping PRC "national champion" firms take over every significant economic and technological sector from their Western competition.

Such institutionalized untrustworthiness is, in fact, an inescapable, *structural* part of the PRC's system of governance. The totalizing nature of CCP authority all but preordains this, for the PRC is a system that precludes true fidelity to the rule of law almost by definition, since national law is merely a creation and instrument of the state, whereas *the state itself* belongs to and works for the Communist Party, which is itself subject to literally *no* legal check unless (and only for so long as) it chooses to be. With the CCP's political legitimacy narrative partly rooted in quasi-Confucian conceits of benevolent omnicompetence but even more strongly rooted in ancient Legalist (and modern Leninist) concepts of brutally unanswerable authority, it rejects democratic accountability to the Chinese people in large part upon the assertion that in return for the Party's absolute power, the CCP's rights-deprived subjects at least live under a collective leadership that is supposedly always correct and always looking out for the best interests of the country. In this context – and for a ruling Party that cannot really evade *responsibility* for anything in China because its absolutism gives it power to *do* just about anything if it wants to – it is hardly surprising the CCP is extraordinarily sensitive about its reputation, and has become notorious not merely for falsifying its own bloody history and record in power, but also for routinely covering up abuses, corruption, and ineptitude on an industrial scale.

But these problems are not new, and Western financial and corporate interests — for years actually encouraged by their governments, sometimes under hubristic delusions about China's neoliberal destiny of peaceable democratic governance that would seem quaint if their modern-day results were not so grim — were long willing to suffer under these conditions in return for the short-term profits offered during the PRC's last generation of export-led growth. As Western governments have begun to wake up to the problems created by such facilitation of the "rise" of an increasingly militarized and brutally authoritarian state that sees its *own* destiny as that of reorganizing the global system around itself, however, the full implications of incautious involvement with the PRC are becoming much more clear.

The United States has increasingly been willing to move against Chinese entities that are engaged in or support some of the more horrific aspects of CCP policy. In the last few months alone, for instance, the U.S. Commerce Department has tightened export control restrictions against Chinese entities implicated in human rights abuses in the implementation of the PRC's campaign of repression, mass arbitrary detention, and high-technology surveillance against members of Muslim minority groups in Xinjiang. The Commerce Department has also tightened export control restrictions against entities involved in helping the People's Liberation Army (PLA) claim and militarize disputed outposts in the South China Sea, which furthered the PRC's illegal claims over that area, while the State Department has imposed visa restrictions on individuals involved in the large-scale reclamation, construction, or militarization of disputed outposts there. The Treasury Department has imposed sanctions against individuals who have been involved in undermining Hong Kong's autonomy and in the CCP's anti-democracy crackdown.

Nor is the question limited simply to dealings with PRC firms in China itself, for the myriad security risks of *any* entanglement with the PRC's technology giants – risks such as user data theft, espionage, vulnerability to cyber criminals, complicity in the human rights abuses of the CCP surveillance state, and risk of strategic and political manipulation from Beijing – are also becoming increasingly clear. This growing understanding of the risks of involvement with PRC firms such as Huawei has prompted leading Western governments such as Germany, France, Japan, Sweden, the United States, and the United Kingdom to impose ever more effective restrictions upon efforts by such firms to take over 5G telecommunications infrastructures around the globe, in some cases simply leading to outright bans on Huawei.

With each step drawing attention to such dangers and increasing the consequences associated with companies' support for or facilitation of provocative PRC policies and activities, Western firms need ever more carefully to consider the dangers inherent in doing business with such

PRC entities. Thus are the de-risking challenges associated with the CCP's domestic totalitarianism and the PRC's destabilizing geopolitical revisionism steadily growing. As awareness grows of these problems, so too do the potential legal, market, and reputational harms that can arise for Western private sector actors from their imprudent entanglement with the CCP Party-State.

And indeed, much of this seems to be underway. In one example – prompted by growing attention being given to the CCP's ongoing campaign of repression against Uyghurs, ethnic Kazakhs, ethnic Kyrgyz, and other ethnic and religious minorities in Xinjiang, including mass detention of more than one million persons, torture, forced labor, coercive family planning (including forced abortion and forced sterilization), sexual assault, and attempts to "Sinicize" exercise of the Islamic faith – Western companies have quite properly begun trying to dissociate themselves from PRC supply chains in the textile sector that might be tainted by forced labor in Xinjiang. Such dis-entanglement seems likely to occur across an ever-broader range of issue areas.

B. Technology-Transfer Risks

Hence, I suggest, the importance of "technology transfer de-risking," or T2D, for in the technology arena there are *additional* risks that deserve attention from private commercial and financial actors: the PRC's ongoing and systematic effort to acquire cutting-edge Western technology and to divert it to the People's Liberation Army (PLA) and the Chinese security services in support of the CCP's destabilizing geopolitical revisionism and hegemonic ambition. Both in this paper series – *e.g.*, *ACIS Papers* 8, 9, 16, and 17 – and in multiple speeches on issues ranging from export control reform to civil-nuclear cooperation and the need to protect U.S. industry against the dangers of entanglement with the PRC's "national champion" technology firms, we have been warning of this threat since at least July 2018. Secretary Pompeo has also spoken forcefully on the topic, specifically addressing his concern to the leaders of the U.S. technology industry.

Simply put, the PRC's strategy of "Military-Civil Fusion" (MCF) presents a significant national security threat to the nations of the democratic world, and an ongoing challenge for any possessor of cutting-edge technology that engages with any person or entity subject to PRC jurisdiction. Irrespective of any end-use commitments or other promises that may have been given, under Chinese law no person or entity subject to PRC jurisdiction can refuse cooperation if the authorities request access to any technology to which that person or entity has access. Nor is there any legal recourse against such commands, for in the CCP's China, the law is *itself* merely a tool of the Party. As noted above, this is simply a fact of life in modern China under the extra-legal – or perhaps, more accurately, *supra*-legal – set of coercive tools available to the CCP:

> "Chinese companies or nationals clearly do not always, or necessarily even usually, act as de facto extensions of the CCP and do its bidding as functional appendages of the Chinese police state. Nevertheless, the CCP and the PRC government apparatus it controls – for, with apologies to Voltaire, who made a similar point about the relationship between 18th Century Prussia and its army, while most states have political parties, the Chinese Communist Party quite literally has its own state – enjoy extraordinary powers to coerce and to co-opt essentially anyone, if the Party chooses to exert itself in such a fashion."

From the point of view of technology-possessors in the non-PRC world, therefore, there is literally no way to be entirely sure that a militarily useful technology, if transferred into PRC hands, will not be diverted to the PLA or the security services. Since the entire MCF bureaucracy exists precisely in order to *carry out* such transfers, moreover, one has to assume that such transfer probably *will* occur. As a result, *any* physical or informational transfer of militarily-useful technology, especially at or near the cutting edge of what is presently possible – not to mention transfers related to foundational and emerging technologies – must be presumed to be problematic. As the CCP regime's oppressive, technology-facilitated totalitarianism at home and destabilizing arrogance and aggressiveness abroad both grow, these facts must necessarily be taken into account in engagements with the PRC technology sector, lest "ordinary" commercial transfers and transactions contribute to *extraordinary* problems that have global implications.

This does not mean, of course, that we should – or could – impose a full-scope *blockade* on absolutely anything that might conceivably have military utility. In a world as interconnected as is our own, we are necessarily primarily in the business of risk mitigation rather than

complete risk avoidance. But it is also clearly the case that much more care and caution is needed in engagements with the PRC technology sector in order to avoid transfers of those technologies explicitly sought by the MCF system (*e.g.*, artificial intelligence, quantum computing, "hot section" aviation engine technology, high-end semiconductor manufacturing technology, nuclear reactor technology, and Big Data analytics), and in order to avoid involvement with PRC entities that support this system. This makes T2D of growing importance.

In the U.S. Government, we have been working to respond to these challenges, beginning with our revision of national security export control policy on civil-nuclear cooperation in October 2018, and more recently with changes in semiconductor design tool licensing, visa screening, and Hong Kong-related export rules, as well as the addition of key PRC technology companies to the Commerce Department's "Entity List." Additionally, we are now revising our rules for screening foreign investments in the United States, and how we handle export control rules vis-à-vis foundational and emerging technologies.

Because technology engagements with the PRC can clearly entail significant reputational, policy, and potentially legal risks, however, it is also now necessary for the *private* sector to pay more attention to technology-transfer de-risking, particularly (though not exclusively) with regard to engagements with the PRC and its MCF apparatus. We are still in the early days of the development of T2D as an area of specialized expertise, but already it is becoming increasingly possible to conduct "know your customer" (KYC) due diligence that can reduce the risk of inadvertent support for or subsidization of the PLA or the Chinese security services. Open-source information, including some very comprehensive analyses by scholars and think tanks, is today making it more and more practical to identify PRC entities that have at least an overt affiliation with the MCF system. Since this is a cooperative challenge, moreover, we in government are working to make more T2D-relevant information available as well.

Private technology-holders necessarily have a good feel for the nature of their own technologies, and therefore also for these technologies' potential implications in malevolent hands. Now that the threat of dangerous technology diversion is so widely known – and is indeed now being comprehensively publicized through various organs of the U.S. Government, even as it steps up measures designed to prevent and to address such activity – private companies have both the opportunity and a clear need to think through de-risking in a new way, to help protect themselves from the multiple risks involved. This is a new area, and despite its importance is still only an emerging sub-specialization within the well-established arena of corporate due diligence. Nevertheless, T2D is a topic of increasing salience, and one should expect to see more work being done in this field.

III. Conclusion

This paper cannot claim to offer comprehensive answers to the challenges of technology transfer "de-risking," but we hope it has at least highlighted the importance, to private sector actors and the government alike, of addressing this need in thoughtful ways. The threats that MCF and the PRC's global ambitions present to the non-PRC world are considerable, and require an effective response. T2D can be an important part of this response, and we look forward to working with our private sector counterparts on this in the months and years ahead.

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.