6月
7月
8月
9月
10月
11月
12月
2019年1月
2月
3月
4月
5月
6月
7月
8月
9月
10月

4

CONSCIOUS DECOUPLING:

THE TECHNOLOGY SECURITY DILEMMA

Darren J. Lim and Victor Ferguson

WHEN PRESIDENT DONALD TRUMP took to Twitter in August 2019 and 'hereby ordered' American companies to look for an alternative to manufacturing in the People's Republic of China (PRC), many scoffed at what seemed like a ham-fisted and unenforceable (and thus typically Trumpian) salvo in the US–China trade war. Reports the following month, however, indicated that the White House was considering delisting Chinese companies from US stock exchanges. The US Commerce Department, citing human rights concerns, but with broader strategic considerations also in mind, announced it would be placing an additional twenty-eight Chinese organisations — including firms specialising in emerging technologies such as artificial intelligence (AI), voice recognition, and data analytics — on a blacklist, effectively prohibiting them from purchasing US components. If 2018 was the year when the world recognised that China had risen as a major technological innovator, in 2019, we learned how the United States intends to respond to this challenge and maintain its technological leadership.

This was the year the concept of 'decoupling' graduated from being an academic talking point to a real-world dimension of the bilateral relationship.[1] Decoupling refers to the process by which the deep economic interdependence binding the United States and China over the past four decades would be unwound, especially (but not exclusively) in high-tech industries. While senior figures in Beijing downplay this prospect as unrealistic,[2] a growing number of Chinese academics warn that it is 'completely possible'[3] and some national security experts in the United States declare it 'inevitable'.[4] Many global business leaders appear to share the last expectation.[5] In the short to medium term, technological decoupling would impose real costs on both economies, not to mention the collateral damage to the existing supply chains of their trading partners across the world. In the longer term and taken to the extreme, decoupling could result in a bifurcation of the global economy, with other states facing a binary choice between US-centred and Chinese-centred alternatives for a growing number of high-tech ecosystems, for the end-use products themselves, as well as the education, research and development (R&D) processes, and supply chains that lie behind them.

At its essence, the decoupling concept falls into the category of policy decisions that involve sacrificing the economic benefits of openness

Made in China
Photo: Martin Abrgglen, Flickr

— flows of goods, capital, people and/or ideas, and information — in the name of other national interests. Invoking a concept developed by security studies scholarship during the Cold War, we argue that China and the United States are caught in a 'technology security dilemma', in which mutual insecurity is driving efforts to decouple on both sides, and that such a trend, despite the economic sacrifices it entails, is likely to persist over the longer term.

Sources of Insecurity

For the United States, decoupling is a consequence of what Washington labels China's 'economic aggression'. The Trump White House cites a broad range of acts undertaken by Chinese commercial actors as well as official economic policies that it claims pose a fundamental threat to US national security and broader economic interests. These include intellectual property theft via industrial espionage or forced technology transfer, extensive state subsidies and other forms of assistance to support 'national champions' in the technology space under Beijing's Made in China 2025 (MIC 2025) initiative, and discriminatory licensing restrictions imposed on foreign firms operating in China. Cumulatively, the argument goes, these actions provide Chinese technology companies with an unfair advantage, while also harming the national security of the United States.

In its 2017 national security statement, the White House claimed that 'economic security is national security'.[6] Linking economic activity with national security is not new; during the Cold War, for example, the United States used export controls to limit the military capabilities of the Soviet Union.[7] What is new is the extensive scope of technology related economic activities deemed to affect national security. It is undeniable that many new technologies designed for consumers can have military applications. The interconnected and technology-driven nature of modern life also leaves a country such as the United States

vulnerable to the hacking of critical infrastructure, cyber espionage, and political interference, through the manipulation of social media, for example. The link between economics and security is further strengthened by the belief that the national security of a leading power will be eroded if it falls behind in technological innovation vis-á-vis a strategic rival, or otherwise loses competitiveness or market share in high-tech industries.[8]

Washington has responded with a broad range of measures to limit or otherwise manage exchange between the two economies. It has introduced tariffs targeting a broad range of Chinese products including industrial technology targeted in MIC 2025. It has tightened restrictions on inward investment and broadened the scope of the Committee on Foreign Investment in the United States (CFIUS) to review and block Chinese investment targeting 'critical technology' and introduced new controls on the export of 'emerging and foundational technologies'. More controversially, Washington has targeted Huawei, ZTE, and other Chinese technology companies, ostensibly for sanction violations and human rights concerns, and indicted a range of Chinese nationals and firms on allegations of industrial espionage.[9] With the possible exception of some tariffs, these measures do not appear to be anomalous manifestations of Trumpism. There is broad bipartisan consensus in Washington for action to address the perceived Chinese threat to US technology leadership.[10]

Beijing, on the other hand, argues that such national security concerns are overblown, misguided, or made in bad faith. The Chinese government believes that Washington's policy responses are not defensive but part of a broader containment strategy designed to slow or stop China's economic development and rightful rise as a science and technology leader. Many in Chinese academic circles share these views.[11] By seeking to limit China's technological advancement, Washington has exacerbated Beijing's perceptions of insecurity.

The Internet: Where Decoupling is Already a Reality

Former Australian prime minister Kevin Rudd has pointed out that decoupling has already occurred online between the two major powers as a consequence of the differences in their political systems.[12] China's construction of the 'Great Firewall' and restrictions on content effectively block the inward flow of politically 'sensitive' information and ideas from the outside world. The Chinese Communist Party (CCP) views a free and open Internet as incompatible with its Leninist Party-state model of authoritarian governance, and potentially a direct threat to its own legitimacy. For China, controlling the Internet is fundamental to national security and public order. This outweighs any potential economic benefits that might be reaped from allowing the likes of Facebook, Google, or *The New York Times* to offer products to Chinese consumers.

Internet regulation illustrates how the Chinese government broadly construes the concept of national security. Anything that undermines the authority or control of the CCP potentially justifies government intervention, even if the economic costs are high. To the extent that the Chinese government enjoys the support of its vast population, this is at least partly due to the country's economic performance.[13] To continue on its successful trajectory and achieve the Party's 'two centenary goals' of becoming a 'moderately well-off society' by 2021 and a 'completely developed country' by 2049,[14] the Chinese economy must develop or acquire the latest technology.[15] The government is therefore extremely sensitive to various kinds of economic disruptions that go beyond more traditional security concerns such as energy security or food security. Thus, measures from Washington that constrain China's technology sector only provide greater incentive for Beijing to strengthen many of the policies that unsettled the United States in the first place.[16]

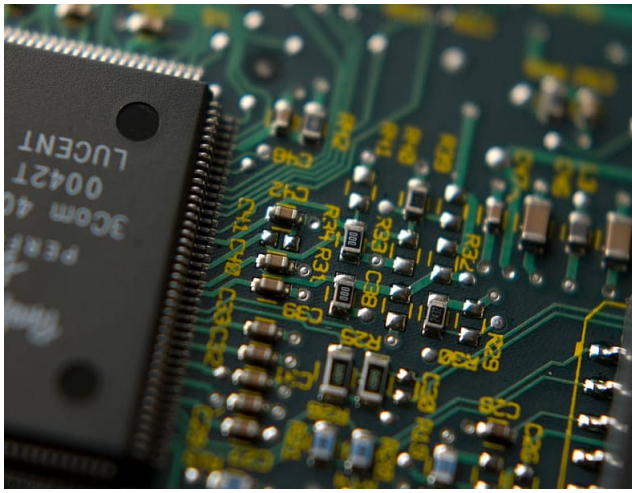
Conceptualising the Technology Security Dilemma

A 'security dilemma' describes a dynamic in which actions taken by one actor to increase its own security are perceived to have the zero-sum impact of reducing the security of another actor.[17] For example, I buy a gun to defend myself. My neighbour, unsure of my intentions, buys a weapon herself, in turn feeding my own insecurity. A rich vein of security studies scholarship posits that, in the anarchic international system, even non-aggressive actions by one state seeking to bolster its security can be perceived by another as decreasing its own. Given the absence of a global sovereign to police and enforce rules, states must guard their own security and question the present and future intentions of others.[18] Under these conditions, relations between two states with peaceful objectives can descend into a spiral of mutual suspicion, mistrust, arms races, and even war.

The concept of 'security' in the traditional dilemma focuses on military power — defence against physical attack and limiting the possibility of domination by coercive military force. Yet the events of 2019 remind us that national security can mean much more, especially to the United States and China, which are now engaged in what we call a bilateral 'technology security dilemma'. Each side is taking measures in the technology domain that it deems necessary and legitimate to safeguard its national security, triggering a spiral of tit-for-tat reactions fuelled by mutual insecurity. Below, we offer two examples of these dynamics.

The first is in semiconductor trade.[19] Despite vigorous efforts to bolster its semiconductor industry over recent decades, China's manufacturing sector remains heavily reliant on advanced chips from the United States and other developed markets, importing approximately ninety percent of its needs annually.[20] In a bid to end that dependence, China has employed a raft of measures, including three that sit at the heart of US concerns about 'economic aggression': industrial policies, including

multibillion-dollar funds for the development of integrated circuits; foreign acquisitions; and, allegedly, industrial espionage.[21] The US government perceives all three of these activities as threats to its national security. The United States objects to the first two because of potential military applications and because it fears ceding technology leadership to a peer competitor. As for the third, the United States perceives such theft as being at odds with global rules, damaging to its own ability to control and profit from American technological innovation and, for some technologies, a direct security concern.



Technology: the security dilemma
Photo: pxfuel

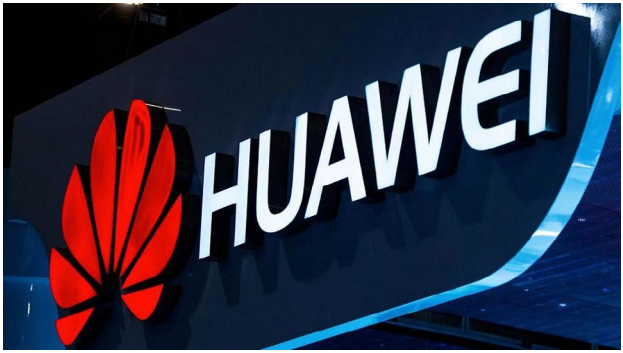
As noted above, the United States has responded by blocking acquisitions, issuing indictments, and banning US companies from trading with Chinese chipmakers, including ZTE (in April 2018) and Huawei (in July 2019). The Trump administration has wound back or delayed some of these measures, but they continue to have serious impacts on companies such as ZTE, which some claim would have folded had Trump not lifted his three-month ban on the company in July 2018.[22] Huawei's future remains unclear, and other firms are reeling,[23] though patriotic consumers in China are reportedly ditching their iPhones for Huawei smartphones.[24] But the sanctions are not having the intended effect. Rather than reining in the behaviour that Washington deems threatening, the Chinese government has doubled down on its quest for self-sufficiency.[25] This,

in turn, reignites US concerns, exemplifying the spiral dynamics of a security dilemma.

A second example of the technology security dilemma arises from the links between the Chinese state and China's key technology firms. Part of China's growth strategy is to build and support 'national champions', encouraging them to 'go out' and compete in international markets. Such state support — which can take the form of subsidies, loans, and cheap finance — is a central pillar of MIC 2025.[26] Huawei is the perfect example of a national champion. Though Huawei is privately owned, state support has helped it grow to become a global industry leader in 5G and telecommunications infrastructure.[27] But influence over such companies that the state exercises in return raises the prospect that Beijing could direct a company such as Huawei to do its bidding — for example, by using its technical capabilities to spy on targeted foreign actors or entities.[28] The close links between Chinese technology firms and the state, and indeed the possibility that national champions with global operations might one day become Trojan horses for surveillance and interference, have generated national security concerns for the United States and allies such as Australia, explaining their reluctance to allow Huawei to run their 5G networks.[29]

Some Western commentators have described measures to deny Chinese technology firms market access as efforts to 'cripple' or 'crush' them.[30] As with semiconductors, China's response has largely been to boost its support for national champions — reasserting the central role of the state in the economy, consolidating state-owned and private enterprises in strategic areas,[31] and further supporting leading firms in a range of technology sectors, from 5G to artificial intelligence to semiconductors.[32] As the connections between the state and Chinese tech firms increase, so do security fears among Washington and its allies.

These dynamics present daunting challenges for policymakers. The literature that deals with military security dilemmas suggests that, if the competing states want to break the cycle, they need to reassure each



US companies ban trading with Chinese chipmakers including Huawei
Photo: VistaCraft Flickr

other about their own non-aggressive intentions.[33] The challenge is to apply these insights to the technology sphere. What, for example, is the analogue of an arms control agreement in the trade and investment space as it relates to the development and use of new technologies? How can each side be made to feel more secure in this issue area?

Pathways to Reassurance

Both Washington and Beijing need to understand the reasons for the other side's insecurity in the technology domain and take steps to relieve these concerns. For Washington, this would mean recognising Chinese worries about reliance on foreign — in particular, American — suppliers of core technologies and components such as semiconductors. Speaking in 2016, President Xi Jinping stressed that 'the fact that core technology is controlled by others is our greatest hidden danger'.[34] Discussing AI in 2018, Xi similarly emphasised the need to reduce 'external dependence for key technologies and advanced equipment'.[35]

How might the United States provide reassurance regarding these concerns? It could try to send a credible signal that it will not interfere with the operation of global markets that supply Chinese firms. This would see the US government revive the tradition of what John Ikenberry

calls 'strategic restraint': binding itself more tightly to institutions that would limit its ability to exercise power over markets and international supply chains.[36] This would likely require the United States to agree to be bound by some kind of enforcement mechanism, akin to the World Trade Organization's compulsory dispute-settlement regime, and invite third parties, such as the European Union and Japan, to monitor and enforce compliance. Given the current scepticism towards multilateral institutions displayed by the White House, an alternative would be to bind itself with domestic institutions — that is, pass laws through Congress to provide greater clarity and transparency regarding any market interventions on grounds of national security.

On the other side of the Pacific, reassurance would similarly involve the Chinese government acknowledging Washington's own concerns, including that with regard to the link between the state and firms such as Huawei, ZTE, Tencent, and Baidu.[37] Exploring credible ways through which Beijing could limit state influence over these companies might send reassuring signals to Washington. For unlisted companies such as Huawei, a public listing on a US stock exchange, which subjects the company to stringent reporting requirements, might be an effective confidence-building measure. Steps to increase transparency regarding

There are concerns in Washington about the link between the Chinese state and companies such as Baidu
Photo: Jon Russell Flickr

such companies' governance structure and operations, such as agreeing to submit to Organisation for Economic Co-operation and Development (OECD) reporting standards and install independent directors, might also prove effective.[38] Licensing locally developed Chinese technology for use by non-Chinese firms — an idea recently floated by Huawei's founder Ren Zhengfei 任正非 with regard to 5G — might also enable Chinese companies to continue growing and competing in Western markets without raising undue concern.[39]

Conclusion

These pathways to reassurance are not necessarily realistic policy proposals given the current state of bilateral relations between China and the United States. But they do help illuminate our diagnosis of the technology security dilemma. Our argument is that decoupling, and the damage it could impose on the global economy, results from mutual insecurity. To arrest this alarming trend, policymakers in Washington, Beijing, and other capitals caught in the crossfire must find creative solutions to make both sides feel more secure.

If neither side is willing to be proactive in seeking to reassure, it is likely that the process of decoupling itself will alleviate some of these pressures over the medium to long term. What has already happened in the online world might point the way.[40] To the extent, for example, that decoupling forces Chinese companies to develop fully independent technology supply chains, vulnerabilities generated by US export controls and other restrictions will dissipate. And if Chinese and American technology companies were to be completely shut out of each other's markets, and those of states falling within each side's sphere of influence, concerns about what those companies might do on behalf of their national governments will similarly recede.

Such broad changes may occur due to continuing government efforts to regulate bilateral trade and investment.[41] At the same time, actors in the private sector may independently decide to reduce their exposure to political risk in foreign markets or other uncertainty created by strained bilateral relations. US firms may even do so because China's cost advantage is diminishing over time as labour costs and regulations increase. At the time of writing, some estimates suggest that, since the advent of the trade war, approximately thirteen percent of US companies with operations in China have shifted or plan to shift some or all of their activity out of the country.[42]

There is perhaps a middle ground between the devastating long-term costs of decoupling and the leap of faith required by reassurance. The two major powers could engage in a focused dialogue about the areas in which they feel most vulnerable to take steps towards mutual reassurance. Brookings Institution Senior Fellow Thomas Wright suggested as early as 2013 that one area in which such an arrangement might prove valuable is information technology and telecommunication networks.[43] Mutually limiting access to specific industries in that space or others that involve 'critical technologies' would be a good first step.[44] Other areas of economic interdependence that are mutually beneficial and not perceived to create significant vulnerability, such as agriculture or merchandise trade, might then continue unimpeded, avoiding a costly, full-scale unwinding of supply chains.[45] Such an agreement would produce a form of 'selective decoupling'[46], or what others have called 'managed interdependence'.[47] This 'conscious decoupling' could be formalised in a treaty — an economic equivalent to the strategic arms limitation treaties negotiated by the United States and the Soviet Union in the 1970s.

There are obvious difficulties, however. For example, even if areas of potential insecurity are identified, the challenge would be to agree on mutually acceptable rules, and on establishing a mechanism to enforce them. This would require the dedicated, ongoing, and creative

involvement of third parties. Given such high stakes, one would hope that all parties could overcome their likely insecurities about the process itself, to avoid an outcome that will ultimately benefit so few.

This text is taken from *China Story Yearbook: China Dreams*, edited by Jane Golley, Linda Jaivin, Ben Hillman and Sharon Strange, published 2020 by ANU Press, The Australian National University, Canberra, Australia.

doi.org/10.22459/CSY.2020.04