Dueling tech regulations and escalating tensions on cross-border transactions

The United States is taking a 'whole-of-government' approach to ensuring that in the economic and military tussle with China, it will prevail – which goes beyond implementation of sanctions and export controls. As China starts flexing its own legislative muscle, multinationals are caught between the proverbial rock and a hard place. Caroline Brown and Evan Chuck describe the terrain and assess appropriate responses.

The past several years have seen seismic shifts in both the world's ability to harness technology and the geopolitics of a post-Cold War economy. What has emerged is the establishment of a new cold war rooted in tech and trade between the world's two major economies. Accordingly, an array of headline-grabbing issues surrounding information and communication technologies ('ICT') have become front and centre in the narrative surrounding the decoupling of the United States and China.

The Cyberspace Solarium Commission (the 'Commission'), tasked in 2019 with identifying a strategic approach for the United States to defend itself in cyberspace, unsurprisingly has been vocal over its concerns surrounding China. In an October white paper addressing how the US might shore up its ICT supply chain, the Commission unequivocally stated, '[P]ut bluntly, in the context of the supply chain for ICT, the US has a China problem.'

The Commission laid out its concerns over Chinese state-owned enterprises taking hold of the market for emerging tech and enabled through a multiplicity of tools, including government policies that bolster the government's role in business transactions, cyberespionage, and significant investments in research and development.

Perhaps the most high-profile example of the dichotomy between the two world powers is seen in the context of the Chinese telecom firm Huawei and 5G, which, due to its significant impact on the US economy and its national security, has taken centre stage in the international technology competition. Along with its greater functionality and usability, which will enable things like autonomous vehicles and will allow for millions of end-user devices to be connected at any given time, 5G has significant national security considerations in addition to commercial ones. Those include both the race to develop and deploy 5G technology and concern over new vulnerabilities as a result of the exponential increase in the amount of sensitive information trafficking the networks, which informs the calls for trusted technology in the telecommunications system.

The Commission highlighted 5G as a critical turning point, going so far as to state that the 'the country that holds the keys to the network holds the keys to the next 20 years of innovation and economic growth and prosperity.' In other words, 5G is a big deal to the US thanks in no small part to the opportunities it presents to itself and to its economic rival, China.

The US government has responded using a whole-of-government approach to ensure that the US is at the cutting edge of this emerging technology and sufficiently protected from threats posed by adversaries. Motivated by current events, including the Covid-19 pandemic, and growing concern about China's own trade and technology practices, regulations and trade

controls, particularly those in the name of national security, have been rapidly evolving at an almost unprecedented rate and that's likely to continue in the next administration.

The US government has sharpened and honed its available tools in order to restrict the flow of technology to China, expanding export controls; bolstering the authorities of the review bodies that protect critical infrastructure from foreign investment and supply chain compromises, namely the Committee on Foreign Investment in the United States ('CFIUS') and Team Telecom; and moving forward legislative proposals that seek to re-shore certain global supply chains, particularly semiconductors. Not only is the US government tapping into and strengthening authorities that have been on the books for a while, but it's also exploring new ways to protect supply chains and sensitive data, including through the issuance of executive orders that establish new regulatory regimes targeted at the ICT and bulk-power energy supply chains. Moreover, existing authorities are being used in novel ways, such as the executive orders aimed at the TikTok and WeChat mobile applications (the implementing regulations of which have been temporarily enjoined by court order) and the more recent executive order prohibiting securities transactions in designated Communist Chinese military companies.

Critical infrastructure: CFIUS and Team Telecom

Recent reform has galvanised instruments that aim to protect critical infrastructure from what has been termed 'the weaponisation of investment'. The passage and implementation of the Foreign Investment Risk Review Modernization Act broadened the scope of review of CFIUS. Most foreign investments in a US business now require some degree of risk analysis to determine whether a deal triggers a mandatory filing to CFIUS or could receive CFIUS attention, even post-closing. This is especially true for deals involving China, which are likely to receive some sort of scrutiny either before

or after closing, particularly those involving the collection or maintenance of sensitive information and emerging technologies.

Similarly, recent actions have bolstered a lesser-known review body. An April executive order enhanced the authorities of Team Telecom, formally known as the 'Committee on the Assessment of Foreign Participation in the United States Telecommunications Services Sector'. Team Telecom is the multi-agency group that assesses national security implications of certain Federal Communications Commission ('FCC') licences, including subsea cables, satellites, and foreign telecommunication connections. The broad scope of Team Telecom's role in the ICT discourse has been made clear in its recommendations to the FCC to revoke or deny certain authorisations of Chinese-owned telecoms, including China Mobile, China Telecom, and an undersea cable that would directly connect Los Angeles to Hong Kong.

Regulatory scrutiny of foreign investment in the United States has been steadily growing for several years, a trend unlikely to change in the near-term given the bipartisan support for the expansion of both review bodies. It's in part due to increased engagement between CFIUS and US allies that other jurisdictions are evaluating their own foreign direct investment review regimes, as demonstrated by The National Security and Investment Bill in the United Kingdom, which could mean increased scrutiny for foreign acquisition of UK companies in sectors such as artificial intelligence, autonomous robotics, and quantum technologies. [See page 28.]

Supply chain executive orders

Long-existing concerns over the security of inbound products and technologies from China and outbound products and technologies exported to China have manifested in a slew of executive orders. While supply chain concerns play out in US government contracting prohibitions, where companies essentially have to choose between sales to the US government and reliance on Chinese supply chains, they go beyond government contracting as well.

In May, the President signed a new executive order declaring a national emergency regarding threats to the US bulk-power system and broadly prohibiting 'bulk-power system electric equipment' where the transaction involves property in which any foreign country or national has an interest. Depending on how it's implemented, the order has the potential to significantly disrupt the supply chain for electrical equipment for US bulk-power systems, which include items used in electric generation projects and transmission systems.

The order closely mirrors one issued almost a year prior in May 2019 directed to the ICT supply chain. That order included very similar language and directed the Commerce Department ('Commerce') to develop regulations to prohibit transactions involving that supply chain produced by 'foreign adversaries' that pose risks to US national security. The November 2019 proposed rulemaking would allow Commerce to require mitigation, prohibition or an unwinding of such transactions. If implemented, it would empower Commerce to identify, assess, and potentially prohibit or otherwise 'address' information and communications technology and services transactions that are determined to present an undue risk to critical infrastructure or the digital economy in the United States, or an unacceptable risk to US national security or the safety of US persons.

Export controls and sanctions

Many companies are also finding their supply chains compromised through an increased use of export controls to guard against perceived threats to national security. The Department of Commerce's Bureau of Industry and Security ('BIS') continues to add to its Entity List, a powerful tool that generally cuts off listed companies from US exports, reexports, or transfers of items subject to Export Administration Regulations ('EAR') absent a licence. BIS's reach is demonstrated through its efforts to limit Huawei's control of the semiconductor industry. Last year, BIS added Huawei and 114 of its affiliates to the Entity List. In May, BIS amended the Foreign Direct Product Rule to further restrict Huawei's and its non-US affiliates' access to US technology or equipment used by semiconductor manufacturers outside the United States, leaving companies confronted with a choice between US-origin technology and equipment integral to advanced semiconductor manufacturing, or Huawei, the world's largest supplier of telecom equipment. Other amendments have extended the military end-use/user rule to include any Chinese person or entity 'whose actions or functions are intended to support military end-uses'.

CHINA HAS ENACTED ITS OWN SET OF TRADE CONTROLS THAT FURTHER REDUCE CHINA'S RELIANCE ON IMPORTED TECHNOLOGIES, PARTICULARLY US ONES, PARTIALLY IN RESPONSE TO US ACTIONS AIMED AT HUAWEI.

While not directly related to ICT, other actions stemming from concerns over human rights and democracy shore up support for tech- and trade-related controls targeted at China. The President signed the Hong Kong Autonomy Act into law in July, accompanied by an executive order that implements many of its provisions. Taken together, the Act and the order create a new Hong Kong/China-related sanctions programme that targets non-US persons making 'material contributions' to the failure of China's government to uphold its obligations under the Joint Declaration and Basic Law, the law that codified China and Hong Kong's 'one country, two systems' paradigm. Along with the recent Uyghur Human Rights Policy Act and designations against Chinese companies under existing authorities, such as the Magnitsky Human Rights Accountability Act, they also can be understood as part of the emergence of a broader sanctions policy targeting China.

China's strategic moves in high technology

China's ICT market is among the most dynamic sectors in China's economy. According to the global market intelligence firm International Data Corporation, the ICT market in China is expected to reach $711.1 billion in 2021, up 9.3% from 2020. China's expenditure on digital transformation is estimated to reach $1.5 trillion between 2021-2024, with an average annual growth rate of 17%. As of 2025, the digital economy is expected to account for 70% of the country's gross domestic product, boosted by new infrastructure and strategies aimed at technological self-reliance.

In addition to its expenditure of funds to achieve its own technology goals, China has enacted its own set of trade controls that further reduce China's reliance on imported technologies, particularly US ones, partially in response to US actions aimed at Huawei. For the first time in nearly two decades, China is revamping its export control regime. On 28 August 2020, China's Ministry of Commerce ('MOFCOM') and Ministry of Science and Technology added to the list of technologies subject to export controls. These changes could have significant impact on multinational companies, including e-commerce or mobile application businesses that rely on data analytics. China's Export Control Law, which combines concepts from more than a dozen existing Chinese laws and related regulations, covers tangible goods (such as dual-use items

and military products) and key related technologies and services. The law, effective 1 December 2020, essentially creates a blacklist management system that includes authorisation to prohibit export of certain controlled items to any specific destination, country, region, or to any specific entities or individuals. Several provisions of the law require additional clarification, including its extraterritorial reach and its corresponding impact on the transfer of technology to non-Chinese individuals, whether in China or abroad.

Separately, China issued regulations in September on its 'Unreliable Entity List' framework. While no company has been placed on the list, the regulations empower MOFCOM to launch investigations against foreign companies acting against China's 'national sovereignty, security, and development interests'. MOFCOM also has the power to impose draconian penalties, including blacklisting an entity from the ability to conduct trade and investment in China, and has wide discretion in deciding if and when to delist companies.

China also issued a draft Personal Information Protection Law in October, which seeks to impose restrictions on entities and individuals, including those operating outside of China, that collect and process personal data and sensitive information on subjects in China. If finalised, this law would complement China's existing cybersecurity law, which requires certain data to be stored within China and network operators to submit to government security checks, and China's draft data security law, which aims to regulate data transfers, including cross-border transfers that could have national security implications for China.

What are multinational companies to do?

Stuck between the dueling tech regulations are multinational companies seeking to maximise opportunities in the world's biggest markets while complying with an increasingly Byzantine maze of regulatory requirements on both sides. Many of these companies, for which China is too large a market to ignore, face a vexing question: How do multinationals maintain or grow business in China but not lose valuable markets in the US, UK, and the European Union as the United States and China continue to decouple?

Answering this question usually involves taking a hard look at where and how goods are manufactured and how services are developed and distributed, including the extent to which companies use outsourcing and offshoring. In many cases, technology services are commonly provided across multiple jurisdictions under the assumption that there are little or no barriers to cross-border exchange of data and technology. China's existing and proposed laws surrounding data access and storage change that fundamental assumption, essentially placing roadblocks on the free flow of information in ways that might disrupt a company's operations in or involving China. For example, these laws might affect a company's development centre in China where routine collaboration with colleagues regarding new designs occurs or impose restrictions on companies that use data analytics, even when that data is as integral to operations as information regarding a company's workforce in China.

Long-standing preferential treatment in China for Chinese companies also hinders business operations of multinationals. Chinese companies that buy from multinational companies have started using the strategic Made in China 2025 policy to send a message to multinational companies: If you want to keep or grow business in China, consider restructuring typical foreign parent-local subsidiary corporate holding structures to reflect more Chinese ownership and control. At times, Chinese multinational companies have used 'soft' pressure on foreign multinationals to accept equity investments from Chinese companies into critical parts of a foreign multinational company's supply chain subsidiaries or affiliates.

As a new administration dawns in the United States, the complexities of US-China relations will likely continue to increase

The many trade controls in the US also serve as reminders that the US government is taking an expansive view of what it's concerned about, underscoring that companies need to remain nimble and versatile in order to comply with new regulations and directives. In addition to a robust compliance programme, companies should maintain visibility into those areas where they might have a nexus to China in order to respond.

Taken together, these developments present multinationals with tough compliance challenges. China's aforementioned Unreliable Entity List, which seems designed to make it difficult for multinationals to operate in China, could result in companies finding themselves in the unenviable position of complying with US sanctions and export controls at the expense of being listed. Such inclusion could have devastating effects, including restrictions on a company's ability to invest in China or even to move its employees around the country.

The ways in which continued changes to both the US and China regulatory regimes could impact the competitiveness of US and other multinational companies operating in China might prompt companies to think about alternatives through a broader 'China Plus the Rest of the World' strategy. As part of that strategy, companies might consider how to change existing supply chains and business and corporate structures in order to mitigate the risks of increasing cross-border regulation while pursuing growth strategies across all major markets. Such an assessment should take into account multilateral and bilateral trade agreements, such as the new Regional Comprehensive Economic Partnership among 15 Asian countries, including China, and cross-border corporate law and tax treaties in order to formulate alternatives that optimise business opportunities while mitigating risk.

As a new administration dawns in the United States, the complexities of US-China relations will likely continue to increase – raising complex, related policy, business and legal considerations that multinationals will need to consider strategically as they review opportunities and challenges in the world's largest and dynamic marketplaces.

Caroline Brown is a partner at Crowell & Moring and a former official at the US departments of Justice and the Treasury.
Evan Chuck is a partner at the firm and head of its Asia practice.
Aurora Zhang, an associate at Crowell & Moring's Shanghai office, contributed to this article.

WWW.CROWELL.COM