Technology Controls & Supply Chain Security – the Linchpins of the New Cold War

Author Robert Shields

By Robert Shields

The United States is heading into a Cold War with China. While the previous Cold War between the US and the Soviet Union featured missile deployments and nuclear standoffs, today's Cold War involves a proliferation of advanced IT systems and an expanding cyber threat landscape. Within this new paradigm, the administration of President Donald Trump aims to maintain the US military and economic edge against China by promoting two key efforts: keeping vital technologies out of Chinese hands, and protecting domestic supply chains from Chinese cyber threats.

This article assesses how the Trump administration is employing these two strategies to "win" the new Cold War, and also warns that these efforts could also undermine US values, if not carefully implemented.

The 5 Domains of US-China Competition

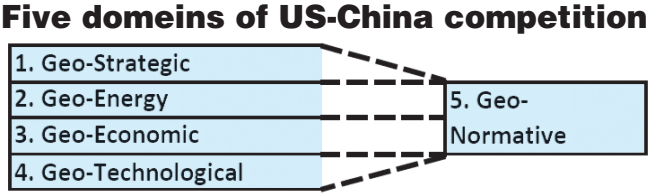
The new Cold War between the US and China is a multi-domain competition for global leadership, security, and wealth. This competition can be divided into five broad domains: geo-strategic; geo-energy; geo-economic; geo-technological; and geo-normative. These domains are overlapping and interrelated, with the geo-normative domain serving as the linchpin across the competitive landscape. Combined, the emergence of these five domains of competition is creating a wide-ranging and complex new Cold War *(Chart)*.

While the first three domains fall along traditional lines of competition, this article focuses on the last two domains, which are becoming increasingly vital to the future of US-China relations:

- "Geo-technological" means the race to develop and mature emerging technologies such as artificial intelligence (AI), fifth-generation wireless networks (5G), unmanned systems, quantum information sciences, and more; and
- "Geo-normative" means the competition to spread each country's values and norms across the globe. In essence, the US seeks to promote "Western democratic values", while China offers an alternative model of authoritarian governance and "state-led capitalism".

CHART

Five domeins of US-China competition



Source: Compiled by the author

Chinese Advances Have Spurred the Geo-Technological Competition

The US has long enjoyed global supremacy in the geo-technological domain. Over the two past decades, however, China has significantly accelerated its technology research and development (R&D) efforts, and appears to be catching up to the US. According to the Center for Strategic and International Studies (CSIS) China Power Project, China increased its R&D spending from $13.4 billion in 1991 to $410 billion in 2016 (in constant 2010 US dollars) – second only to the US, which spent $464 billion on R&D in 2016.

China's R&D spending increase has translated into notable gains in several technology sectors. For example, a March 2019 report by Carissa Schoenick of the Allen Institute for AI concluded that China is overtaking the US in the number of AI research papers submitted and published, as well as the number of "high-impact" AI research papers published. Schoenick projects that China will likely surpass the US in terms of top-10% papers by 2020 and top-1% papers by 2025.

Moreover, according to the November 2018 publication of the "TOP500" list of supercomputers, 227 of the world's top 500 supercomputers (45% of the global total) are Chinese, while the US has 109 top 500 supercomputers (22% of the global total). The US still maintains a slight edge over China with respect to aggregate system performance at 38% of global performance, compared to 31% for China. However, this gap is narrowing *(Photo 1)*.

Beijing has also positioned itself to overtake the US as the global leader in other key technology sectors over the next decade. Major Chinese government policies have outlined this vision. For example, in 2008, Beijing established its *"Thousand Talents Program"* to recruit top international scientists and researchers to work on advanced scientific and technology projects in China. In 2015, Beijing released *"Made in China 2025"*, a series of state-led initiatives aimed to promote key Chinese technology sectors, such as IT and advanced manufacturing. Beijing has also promoted more sector-specific advanced technology initiatives. For example, the 2017

"Generation Artificial Intelligence Development Plan" aims to make China the world leader in AI by 2030.

Beijing's Technology Policies Are Threat to US

Beijing has fueled its technological advancement through an extensive campaign to transfer technological knowledge from the US to China – using both licit and illicit means. The most comprehensive account of Chinese technology transfer activities was a March 2018 report by US Trade Representative Robert Lighthizer entitled *"China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation"* (which was later updated in November 2018). This report found that China uses a number of legal ways to transfer vital technological knowledge and intellectual property from the US to China, such as targeted investments and joint ventures into the US. It also found that China engages in a number of legally dubious technology transfer activities, such as the imposition of forced technology transfer requirements on US companies investing in China, as well as illegal activities such as cyber intrusions.

Chinese law also stipulates that its citizens and companies must conduct espionage against foreign entities if asked by the Chinese government. Specifically, the Chinese National Intelligence Law of 2016 requires all Chinese persons and companies "to support, provide assistance, and cooperate in national intelligence work". As such, Beijing can require any Chinese citizen or company to steal technology and intellectual property from a US counterpart.

United States Bolstering Controls on Critical Technologies

There is a growing consensus in Washington that Beijing's technology advancement initiatives and technology transfer practices are a threat to US economic and security interests. In response, the Trump administration has taken several actions to address China's activities in the technology realm. However, these actions are not articulated in any one comprehensive policy document or initiative. Instead, the Trump administration is engaging in a reactive campaign to address the rising Chinese technological threat.

Tighter controls on sensitive US technologies are a key pillar of the Trump administration's ad hoc campaign to address this threat. As background, the US Commerce Department's Bureau of Industry and Security (BIS) is a key government office managing US export control regulations. BIS places controls on exports that are deemed vital to the US military or to US national security interests. The US government also closely monitors foreign investments into US businesses. Specifically, the Committee on Foreign Investments in the United States (CFIUS), an interagency panel led by the Treasury Department, prevents foreign acquisitions of US entities that could result in the transfer of vital military technologies outside of the US.

Photo 1: "ORNL Launches Summit Supercomputer", Oak Ridge National Laboratory, June 8, 2018
https://www.ornl.gov/news/ornl-launches-summit-supercomputer

IBM Supercomputer Summit at Oak Ridge National Laboratory

In August 2018, Congress and the Trump administration used the annual military authorization bill, the Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA), to address the growing Chinese technological threat with provisions aimed to reform the BIS export controls regime and update the CFIUS process.

First, as part of the FY 2019 NDAA, the Export Control Reform Act (ECRA) required the Commerce Department to create an interagency group to develop new export controls on emerging and foundational technologies that are deemed "essential" to US national security. Though not explicitly stated in the law, China is the target of these new export controls. Indeed, the bill's sponsor, now-retired Republican Representative Ed Royce of California, said that Chinese technology transfer threats were the key impetus for the ECRA.

BIS is currently working with US industry to finalize the new export controls. So far, it has identified a number of emerging technologies that require additional export controls in diverse fields such as AI; position, navigation, and timing; advanced computing, quantum information and sensing; and robotics, additive manufacturing, and data analytics. BIS is expected to finalize the first round of new export controls based on these emerging technologies in the coming months. It will also soon identify foundational technologies that require export controls *(Photo 2)*.

BIS has also added a number of Chinese firms to the "Entity List" – an export control list that precludes US companies from exporting to certain foreign entities (with limited exceptions). Since 2018, BIS has added nearly 70 Chinese entities to the Entity List – many of which are high-tech companies. For example, in October 2018, BIS

Photo 2: "Image Library – GPS III satellite", GPS.Gov, March 5, 2019 https://www.gps.gov/multimedia/images/

GPS-III Satellite

added Chinese state-owned semiconductor company Fujian Jinhua Integrated Circuit Co. to the Entity List. Trump has also ordered major Chinese telecommunications companies ZTE and Huawei to be added to the Entity List. Although he quickly removed ZTE in 2018 in response to Beijing's pleas, Huawei remains on the Entity List. However, Huawei's designation is a key element in the ongoing US-China trade discussions, and thus could be removed over the course of these negotiations.

Second, and also part of the FY 2019 NDAA, the Foreign Investment Risk Review Modernization Act (FIRRMA) enacted a number of CFIUS reforms aimed to block certain investment in US industries deemed critical to US national security. In particular, FIRRMA expanded the authority of CFIUS to review proposed investments by foreign entities into companies that deal with critical technologies, critical infrastructure, or sensitive personal data. FIRRMA also gave CFIUS authority to conduct stricter oversight of foreign purchases of real estate located near sensitive US assets or facilities. Like the ECRA, these CFIUS reforms target Chinese investment. The bill's sponsor, Republican Senator John Cornyn of Texas, said that the purpose of FIRRMA is to harden US defenses against foreign acquisitions by China and other potential adversaries. CFIUS is currently running a pilot program implementing these changes.

Even without FIRRMA's reforms, CFIUS has been active in recent years in protecting US chip manufacturers – a key enabler of emerging technologies – from Chinese investors. For example, in 2017, Trump blocked the acquisition of major semiconductor chip maker Lattice Semiconductor by Chinese-backed Canyon Bridge Capital Partners.

Rise of Federal Supply Chain Security Against Chinese Threats

These technology transfer controls and investment restrictions are only one part of the US-China geo-technological competition. Another key aspect is US supply chain security. Indeed, US policymakers fear that the inclusion of certain Chinese companies within US supply chains presents a cyber-espionage threat against the US government, companies, and citizens. Specifically, they believe that Chinese companies could install malware or similar cyber-weapons into Chinese components that enter US supply chains.

To eliminate (or at least manage) these threats, the Trump administration has begun to block certain companies from US federal government supply chains, essentially "decoupling" federal supply chains from a number of Chinese entities. The most widely discussed case is the US government's ban on federal purchases of Huawei, ZTE, and other Chinese technology companies, as required by the FY 2019 NDAA. This provision went into effect in August 2019.

The FY 2019 NDAA also prohibited federal agencies from contracting with or issuing grants to any company that uses Huawei, ZTE, and others as a "substantial or essential" component of their business. This provision is scheduled to take effect in August 2020. However, many US businesses have warned about the provision's broad reach, arguing that it would be prohibitively costly to rid their supply chains of Huawei and ZTE, thus hurting profits and, in turn, the US economy. This provision will be a source of major debate in the coming months as federal agencies try to decide how to implement this law in a way that balances US national security with US business interests.

US Government's Expanded Role in Private Sector Supply Chain Security

The Trump administration is also working to decouple America's private sector supply chain from Chinese entities, as companies struggle to defend against sophisticated cyber-attacks emanating from China (and elsewhere). In May 2019, Trump signed an Executive Order that gives the US federal government broad authority to prohibit business transactions between US entities and

certain foreign suppliers in the information and communications technology (ICT) sector if such transactions are believed to pose an "unacceptable risk" to US national security (i.e., cyber-espionage, malware installations, and other malign cyber activities). Essentially, this Executive Order establishes the basis for future government regulations and other actions to ban certain Chinese companies from the US private sector's ICT supply chain. In particular, it aims to protect 5G networks.

In response to the Executive Order, the Commerce Department is finalizing new rules to create a process that excludes certain foreign products from US ICT supply chains. These new rules are expected to block Huawei and ZTE – among others – from the US private sector ICT supply chain.

Outside of these upcoming regulations, the Department of Homeland Security's new Cybersecurity and Infrastructure Security Agency (CISA) is coordinating efforts among public and private sector stakeholders to protect US critical infrastructure against emerging technological risks. CISA has focused recent initiatives on securing the 5G supply chain, identifying critical risk areas in US infrastructure, and developing strategies to mitigate cyber (and physical) risks to the US. CISA aims to foster deep partnerships with industry and become a close partner with companies that seek to build trusted and resilient supply chains. In fact, CISA is home to the ICT Supply Chain Risk Management Task Force, a group of government and industry stakeholders developing policies to bolster ICT supply chain resiliency *(Photo 3)*.

Trump administration efforts to confront Chinese technology transfers go beyond protecting federal agencies and US industry. Federal agencies such as the Energy Department and Defense Department are engaging in greater oversight of academic partnerships to better protect universities from Chinese cyber intrusion threats and technology theft.

Blurred Lines Between Economic & Security Interests

The above discussion demonstrates that, unlike the previous Cold War, the current US-China competition features a close entanglement of security and economy. Indeed, the US government's campaign to protect critical technologies and defend supply chains has shifted US policymaking away from the "traditional" separation of the economic and security realms.

Notably, export controls are no longer primarily focused on technologies that impact national security-specific interests, like long-range missiles and submarine technology. Rather, the US government's export control regime will focus increasingly on technologies that play a vital role in the US military *and* new-age

Photo 3: "President Donald J. Trump Signs the Cybersecurity and Infrastructure Security Agency Act", The White House, Nov. 16, 2018 https://www.flickr.com/photos/whitehouse/32041940468/

President Donald Trump signs CISA into law.

economy (such as AI and additive manufacturing), representing a shift toward the protection of both national security and (increasingly) economic security interests.

Moreover, the digitalization of every economic sector has shifted the Cold War "battlefield" from nuclear missile silos to private sector supply chains. Every critical economic sector in the US (including energy, financial, and telecommunications) is now dependent upon digital assets and emerging technologies such as AI, 5G, and IoT devices. These sectors are vulnerable to a growing number of cyber and digital threats. US businesses are no match for these sophisticated attacks. Consequently, the US government (led by CISA and the Commerce Department) has become more proactive in protecting private sector supply chains from digital attacks.

The emerging 5G market has become a critical element of the US government's supply chain defense efforts precisely because of its vast economic potential. In fact, a 2017 study by research firm IHS forecasted that 5G will enable $12.3 trillion of global economic output by 2035. That is why the Trump administration sees Huawei's expansion into global 5G networks as both an economic threat and a cyber-espionage challenge. CISA is working to secure the private sector's 5G supply chain in order to ensure optimal security and promote economic growth in this key sector.

Consequences of US Technology Controls & Supply Chain Security

Ironically, these Trump administration actions aimed to defend critical technologies and supply chains against Chinese threats could undermine US economic growth. The expansion of government efforts to protect these sectors can undermine technological

innovation and destabilize business operations. For example, banning certain Chinese companies from US supply chains could force companies to "rip and replace" a majority of their architectures and installations – an expensive proposition. While large companies could absorb such replacement costs, small and medium-sized IT companies may struggle to adapt. In addition, overly broad or vague export controls on emerging technologies like AI could prevent high-tech startups from seeking market expansion abroad or research institutes from collaborating with foreign partners.

Moreover, the growing involvement of the Defense Department, Commerce Department, and CISA within the US ICT sector could possibly create risks for the privacy and freedom of communication for US citizens. In fact, CISA leadership has recently expressed interest in increasing collaboration with the National Security Agency (NSA) to protect the ICT sector (among other critical economic sectors). In the wake of revelations alleging past NSA surveillance of US citizens, any expansion of government oversight into the ICT sector will be met with public concern.

So far, there has been little meaningful discussion in the US about how to defend US technologies while also respecting privacy, freedom of communication, and free-market principles. One notable exception is CISA's August 2019 *"Strategic Intent"* document that states: "Security is not an end unto itself, and efforts to mitigate risks must be appropriately balanced with civil liberties, free expression, commerce, and innovation." While this acknowledgment is a good first step, it must be followed by robust discussions and deliberations by a broad group of stakeholders on how to balance these competing goals.

"Winning" the Geo-Technological Competition Requires Reprioritization of Values

In his 1988 address to Moscow State University, President Ronald Reagan linked the power of emerging technologies to Western values:

"[W]e're emerging from the economy of the Industrial Revolution… in which there are no bounds on human imagination and the freedom to create is the most precious natural resource. Think of that little computer chip… But progress is not foreordained. The key is freedom – freedom of thought, freedom of information, freedom of communication."

Reagan understood that values such as free speech and communications are necessary ingredients to enable technological progress in the US and the world. Without these values, technology can threaten the human condition and undermine progress.

Reagan's message holds true today. What good is an export control regime if it undermines the very free-market economy it seeks to protect? What good are defenses against Chinese cyber espionage if they undermine US citizens' privacy? "Beating" China in the geo-technological competition does not only mean developing and protecting the best algorithms and wireless networks. More holistically, it means developing and deploying these technologies in a way that supports and protects US values of freedom, privacy, and free-market economics. It means winning the geo-normative competition.

The Trump administration should focus on the following policies to achieve both geo-technological and geo-normative goals:

- Commerce should work closely with industry to implement new export controls on China that only target the transfer of emerging technologies with clear military applications. These narrowly defined controls will allow continued US involvement in international R&D efforts to advance technological development.
- Congress and the Trump administration should advance policies that offer tax incentives and similar opportunities to tech companies to help create viable alternatives to Chinese companies. It should also build upon current Trump administration initiatives to promote critical technology sectors, such as the American AI Initiative and "5G FAST" plan.
- At the same time, the Trump administration should limit the scope of Section 889 implementation to avoid collateral impact on small and medium-sized companies.
- The Commerce Department should implement only limited and narrow regulations for the ICT supply chain to minimize risk of major economic disruption.
- Finally, CISA should promote supply chain security by expanding public-private cyber threat information sharing programs and promoting baseline cybersecurity standards across the US private sector. However, CISA should be wary of close involvement with the NSA in these efforts, given public concerns about its allegations of its past operations.

These policy recommendations promote limited export controls and collaborative security measures that would protect the US against Chinese technology threats and adhere to and defend US values. JS

Robert Shields is a manager at International Technology and Trade Associates, Inc. (ITTA), supporting clients on a wide range of issues involving US science and technology policy.