RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 213 – 23 October 2019

Geopolitics and Technology

A Conflict Without End? The US-China Tech War

By Adam Segal

SYNOPSIS

President Trump's campaign targeting Chinese technology companies is motivated primarily by concerns about economic competition and security threats. This has been expanded to include democratic values and human rights. Framing the technology rivalry as one over ideology and political values, however, means the US-China tech war is likely to intensify and expand.

COMMENTARY

FOR THE last two years, the Trump administration has waged a broad campaign pushing back against Beijing's use of industrial policy and targeting Chinese technology companies. In the beginning, Washington's efforts were motivated primarily by concerns about economic competition and security threats.

Over time, however, the United States has expanded the competition to include democratic values and human rights, and US officials and Western analysts have promoted an increasingly expansive and threatening view of the tech sector's relationship to the Chinese Communist Party. As Christopher Ford, Assistant Secretary Bureau of International Security and Nonproliferation, put it:, "On balance the Chinese technology giants are not purely private actors, but instead function as at least de facto tools of the Chinese Communist Party when it matters most."

US Tech Containment

A focus on values leaves little room for compromise and means that there is essentially no limit to where the US will contest Chinese technology development. Some narrow agreements on technology competition between Washington and Beijing based purely on economic and security interests might have been possible.

But this may prove extremely difficult to reach given the high levels of mistrust in the bilateral relationship. Framing the technology rivalry as a competition over ideology and political values as well, however, means that the US-China tech war is likely to intensify and expand.

Since taking office, the Trump administration has highlighted Chinese technologies policies as a danger to US economic and national security. The December 2017 National Security Strategy, for example, described Russia and China as "determined to make economies less free and less fair, to grow their militaries, and to control information and data to repress their societies and expand their influence".

The strategy called out Beijing for the cyber-enabled theft of intellectual property as well as the use of "largely legitimate, legal transfers and relationships to gain access to fields, experts, and trusted foundries that fill their capability gaps and erode America's long term competitive advantages".

In addition, in June 2018 the White House released a report, entitled *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, claiming China used industrial policy, state-sponsored IP theft, forced technology transfer, and overseas acquisitions in order to "access the crown jewels of American technology and intellectual property".

Four-fold Policy Response

In response to what Trump sees as threats, Washington has deployed a four-fold policy response. First, the US levied tariffs on Chinese products, including those benefitting from "Made in China 2025", Beijing's effort to build a smart manufacturing base through low-interest loans, assistance in buying foreign competitors, and research subsidies.

Second, Congress and the White House limited Chinese investment in US technology sectors. The Foreign Investment Risk Review Modernisation Act updated the list of critical technologies that would trigger a security review and allowed the Committee on Foreign Investment in the US to investigate additional investments such as minority positions or overseas joint ventures.

The Trump administration has blocked the sale of Lattice Semiconductor to a group that involved a Chinese venture capital firm; prevented Ant Financial's acquisition of MoneyGram; and demanded that Beijing Kunlun Tech give up their control of Grindr.

Third, Washington has make it more difficult for Huawei and other Chinese telecom companies to do business in the US and other markets. Congress has prohibited the Pentagon from buying network equipment from either Huawei or ZTE, and in May 2019 the Trump administration issued an executive order which provided sweeping

authorities to exclude from the U.S. market information technologies linked to “foreign adversaries.”

Positioning Huawei as a Threat

The Commerce Department also placed Huawei and 68 of its affiliates on a list of firms to which US companies may not sell without government approval. While the Department has suspended the ban twice, and the White House has suggested that it would issue licences to companies to sell non-sensitive technologies to the company, major US companies such as Google and Micron have suspended doing business with Huawei.

Fourth, the Commerce Department has also strengthened the controls on the export of sensitive dual-use technologies, adding, for example, the Chinese supercomputer company Sugon to a list banning them from buying U.S technology due to the company’s research on supercomputers that can be used in military applications.

In October 2019, the Commerce Department added 28 companies and government organs to the entity list, including leaders in China’s AI sector such as SenseTime, Megvii, Yitu, and iFlytek, for aiding the “repression, mass arbitrary detention and high-technology surveillance” in Xinjiang.

Struggle Over Values

As the *New York Times* notes, the sanctions on these companies adds a human rights and digital surveillance dimension to the US strategy. US officials have expressed concerns not only about the deployment of facial and voice recognition technologies within Xinjiang, but also the export of these technologies to developing countries.

In response to a ZTE smart cities project in Argentina, for example, a State Department official argued that “China gathers and exploits data on an unrivaled scale, and uses the information to promote corruption, support arbitrary surveillance, and silence dissent”.

Parallel to this concern about Beijing exporting its digital authoritarianism, US officials have increasingly described the Chinese technology sector as subservient to the demands of the Chinese Communist Party. US analysts point to three developments. First, the Party is reasserting political control over the tech companies through the establishment of party cells within enterprises and by the ownership of shares in key companies.

Second, the National Intelligence Law and Cybersecurity Law appear to subject the companies to invasive demands from the security services for access to data. Third, Xi Jinping has elevated and re-energised Military-Civil Fusion, a national level effort to lower the barriers between the private sector and military industrial base. The end result is technology at the service of the CCP. As Assistant Secretary for East Asian and Pacific Affairs David Stilwell told a meeting of the Committee of 100:

If Chinese officials believe a given technology can be of any use to the country’s military and national security complex as Beijing prepares itself to bully and coerce its

neighbours and challenge the United States for global leadership, one can be quite sure that the technology will be made available for those purposes – no matter what. There are no checks and balances, no independent judiciary, no rights to privacy or free expression to provide recourse.

The demands of a strategy driven by both geostrategic rivalry and ideological struggle against an illiberal and authoritarian power are extremely high: bipartisan efforts to check and contain China across a large number of technologies; broad support for efforts to re-invigorate innovation in the American economy; and close cooperation with allies and friends.

It seems highly unlikely that a Trump administration facing other foreign policy crisis in the Middle East and impeachment hearings at home will be able to bring all these components together. But even incomplete efforts to construct and execute US strategy are likely to result in an expanded tech rivalry with China.

Adam Segal is the Ira A Lipman Chair in emerging technology and national security and director of the digital and cyberspace policy program at the Council on Foreign Relations. He contributed this to RSIS Commentary as part of a series on geopolitics and technology. He tweets at @adschina.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg