How Japan should avoid becoming a loophole for technology leaks to China

Hosokawa Masahiko, Professor, Chubu University

Trump signs China trade deal but the underlying economic conflict does not end

Prof. Hosokawa Masahiko

President Trump signed an initial trade deal with China. As expected, markets seem to have reacted positively to the initial agreement by the two governments. But the tariff fight started by President Trump seems only to be a surface-level conflict between the United States and China. In fact, at a deep level, there has been consistent escalation of the technological power struggle, which is growing more serious within Congress and the Washington policy-making community as a whole. More recently, Washington policymakers have redefined the strategic framework for the US relationship with China from a human rights perspective.

The technological power struggle with China has become so deeply entrenched within the Washington policy community that even President Trump cannot make a deal with China easily without listening to them. Therefore, I believe that the technological power struggle with China will continue over the medium to long-term. It appears that, accordingly, the Beijing Government is ready for a long battle.

Behind the technological power struggle is China's state capitalism, which is incongruent with the so-called Western values that have developed over the years since the end of the Second World War. State capitalism as adopted by China is an economic system designed to drive the governance of the state by the Communist Party. The state-led strategic plan, Made in China 2025, is not just an industrial policy. Under this plan, China seeks to modernize its military while becoming the greatest manufacturing state in the world. The US government seems to maintain a critical approach believing that the US loss of its technological advantage over China would be a major security risk. It should be noted that this is a view not only adopted by the United States, but also by countries in Europe, where there is growing concern regarding China.

America's basic stance toward China is articulated in its National Security Strategy announced in December 2017 and remarks delivered by Vice President Mike Pence in October 2018, both of which have been embodied as specific policies in the National Defense Authorization Act (NDAA) of 2019 and 2020.

A fight to end inter-reliance

A noteworthy aspect of the NDAA is that it defines semiconductors and rare earth elements as core areas of industry in terms of national security.

China is desperate to produce semiconductors domestically and reduce their reliance on US chips. The Made in China 2025 project sets the goal of achieving a self-sufficiency manufacturing rate of 40% by 2020 for its semiconductor industry and 70% by 2025. To achieve these targets, China has been accelerating its strategic activities to acquire technology and recruit manpower with its abundant financial resources.

The reduction of its heavy reliance on China for rare earth metals is an urgent US security need. Their heavy reliance on China for rare earth elements poses a very serious problem because these materials are essential for building missiles and other military equipment. Given this situation, the United States has already begun stockpiling and pursuing the diversification of its sources of rare earth metals.

Meanwhile, China has been strategically working towards increasing its self-reliance in areas including not only semiconductors but also robotics, large airplanes and other sectors included in the list of ten key industries in the Made in China 2025 initiative along with a policy of promoting the domestic production of software, including information systems.

The US-China tug-of-war is particularly tense in the field of telecom infrastructure, which is immediately related to national security. Things are not limited to the battle for 5G supremacy. For example, China has announced the BeiDou Navigation Satellite System, a satellite-based positioning system, aiming to reduce its reliance in telecommunications on America's GPS. Another example is China's aggressive maritime strategy against submarine cables built largely by the United States and its allies, including Europe and Japan.

Furthermore, China is desperate to reduce its reliance on America by moving away from the dollar as a key currency in view of the risks associated with the financial sanctions imposed by the United States. In this respect, key initiatives adopted by China include the One Belt, One Road Initiative, an ambitious global development strategy, and digital currency. The Belt and Road Initiative could also be interpreted as a tool designed to boost the internationalization of the yuan. Digital currency is one of the strategies intended to reduce China's reliance on the US dollar.

As I mentioned earlier, both China and the United States are desperate to escape from their reliance on each other in economic areas related to their fundamental security.

The concept of "economic statecraft" has come into the spotlight recently. This concept refers to the policy instruments used by state governments to achieve strategic geopolitical goals in an economic way, without relying on military power. It appears that both China and the US are actively relying on economic options. It is time for Japan to take a definitive step forward in the face of the economic statecraft practiced by China and the United States.

The partial disengagement strategy of the United States

Partial disengagement between the US and China is a hot topic among Washington policymakers right now. During the Cold War era, the US defense policy against the Soviet threat was focused on containment. At the same time, the United States adopted a policy of engagement with China in the post-Cold War years, expecting a convergence of values between China and Western nations, but this policy failed. With the current globally interdependent economic structure, it is absolutely not possible for the United States to backtrack and adopt a containment policy toward China today.

There are rising fears that the decoupling of the US and China is an irreversible third option for the United States to take, but a full economic decoupling is unrealistic and impossible.

At the same time, the United States' continued naive embrace of free trade regardless of the realities of the security risks associated with China is useless. Given this analysis, it seems that the United States is following a partial disengagement strategy, determining specific areas of sensitive technology directly related to security interests and separating them from China. A US partial disengagement policy will inevitably involve its allies and friendly nations.

For example, the media reported in November of last year that ASML, a leading supplier of semiconductor manufacturing equipment based in the Netherlands, was halting shipments of the advanced equipment needed to make next-generation chips to a state-owned semiconductor manufacturer in China. This was obviously the result of pressure from the Trump administration. It is highly probable that the same kind of pressure from the United States will hit even Japanese suppliers of semiconductor manufacturing equipment as key partners involved in global supply chains. Another symbolic example is Taiwanese semiconductor giant TSMC, which has found itself in the middle of the technology standoff between the United States and China, pressing TSMC to make chips in America or China. Japanese manufacturers supplying components to TSMC will be affected accordingly.

In fact, some Japanese companies have already found themselves torn between conflicting demands. A certain number of manufacturers in Japan found themselves in the middle of the standoff between the United States and Huawei after the Trump administration added Huawei to the Entity List.

Furthermore, China is in the process of creating its own entity list to hit back against the United States. With its own entity list, the Chinese government seeks to impose sanctions on foreign enterprises halting shipments to Chinese corporations in response to the "unreasonable" trade restrictions imposed by the US. It even looks possible that some manufacturers or suppliers will find themselves in the middle of the entity list battle between the United States and China, each requiring compliance with their own restrictions.

"Control of sensitive technology" accelerated by the United States

Keeping in mind the specific sectors using sensitive technologies, the United States is working to step up the control of technology, with efforts consisting of two major initiatives, investment

controls and export controls.

Presented with the threat of China, legislation President Trump signed into law in August 2018 expanded the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) to review transactions and made it more strict, aiming to prevent sensitive technology from leaking to foreign countries through foreign investment in US corporations. Thereafter, Europe adopted strict restrictions of a similar nature for the same reasons.

Since August 2018, the Trump administration has moved to prohibit government contracts for Chinese telecom and video surveillance equipment for security reasons, and even banned private-sector companies from purchasing equipment or services directly from China.

Nearly 200 Chinese suppliers have been added to the Entity List recently, including Huawei and other manufacturers of video surveillance equipment, supercomputers and nuclear power plant facilities. The Trump administration's approach toward China has moved away from simply "do not buy" or "do not use" their products to "blocking their sales" or "not allowing them to manufacture."

With the introduction of the Export Control Reform Act (ECRA), the US government is set to take definitive action to control exports this year, aiming to impose new restrictions on exports of emerging and foundational technologies that have been previously uncontrolled. Emerging technologies include artificial intelligence and quantum technology, while foundational technologies refer to semiconductor manufacturing, etc. The Trump administration is currently working to identify emerging technologies and foundational technologies in further detail. We must keep an eye on any developments in this matter because it will have a significant impact on businesses in Japan.

Export controls as a "new CoCom targeting China"

China's military-industrial complex and National Intelligence Law are key elements for the United States to consider when developing export controls.

Even civil technologies provided to businesses in China run the risk of being diverted to military use with the military-industrial complex that is in place. In other words, making a distinction between civil technologies and military technologies is impossible.

Furthermore, these risks have been intensified by the National Intelligence Law, which requires companies or organizations operating in China to give the government access to any information they need.

Accordingly, it is urgently necessary for countries around the world to review and update their export controls to China. Companies exporting to China have been primarily careful about those products running the risk of being diverted to military use, but this approach no longer seems to be effective. This forms the basis for the US actions to accelerate export controls toward China today.

Given this situation, it is necessary for the United States to take an approach that works to prevent sensitive technology from leaking to China, whether it is for military or civilian purposes.

During the Cold War period, multilateral export controls (known as "CoCom") were established by the Western Bloc aiming to protect and preserve their technological advantage over the Communist world. After the Cold War ended, this export control system began shifting its focus in the 1990s toward preventing the proliferation of military equipment to countries of particular concern. It looks like the historical export control system is beginning to change into a new CoCom targeting China.

The existing international framework of export controls seems to no longer be effective in the wake of China's rise on the global stage. Therefore, the United States acting alone to implement restrictions would be of limited effectiveness. It appears inevitable that the US will look to its allies, including Japan, for international cooperation. I believe that recent developments like this suggest the looming possibility of a new international trade control scheme to be established under the leadership of Japan, Europe and the United States.

Horrifying "shadow laboratory"

Another important point for the United States to consider in its Chinese export controls is the prevention of leaks of sensitive technology currently under development. University research labs across the US are targeted by the Chinese government as a primary source of technology, and the US government is working quickly to respond to this.

In 2008, the Chinese government launched the Thousand Talents Program, aiming to recruit leading international research experts, mostly Chinese scientists doing research in the United States. However, this program fuels US suspicions about organized activities to steal sensitive technologies from the United States.

A Chinese scientist at Duke University was in the news recently regarding these concerns. It was reported that he stole intellectual properties related to a Pentagon-funded research project creating an invisibility cloak metamaterial and took them home to China, which sponsors his research activities today.

"Shadow laboratory" is the term often used to refer to organized activities by the Chinese government to spy on technologies abroad. They build a research laboratory in China that copies exactly the intellectual property they have obtained from their spy activities abroad.

Amidst this, the Trump administration is considering tighter visa controls on students and researchers coming from China, and intensified voluntary controls are being adopted at universities across the United States. An increasing number of universities have refused to accept offers of funding from Huawei, suspending joint research projects with them.

Japan as a loophole for tech leaks

Facing this environment, Japan must not become a loophole for leaking technology, and the government must move quickly to close institutional loopholes. With the economy and national security connected together even more closely than before, the concept of economic security has become increasingly more important. The Japanese government most improve its technology

controls, including investment and export controls.

The Diet has recently passed legislation that amended the Foreign Exchange and Foreign Trade Control Law, prompted by moves by the United States and European countries announcing stricter investment controls for security reasons in view of China's rise. With this legislation, Japan is finally equipped with investment controls corresponding to those already adopted by the US and Europe. But this is not enough. CFIUS has carved out exceptions only for Australia, Canada and the UK due to certain aspects of their robust intelligence-sharing relationship.

Furthermore, Japan must step up its export controls extensively with an eye on any moves the United States may make in the future. It seems necessary for Japan to work closely with Europe, aiming to reach a consensus approach and establish a new export control system targeting China under the leadership of Japan, Europe and the United States.

It is also important for Japan to work strategically without failing to analyze the wide spectrum of technology controls from a broad perspective. At the same time, Japan must comprehensively examine the variety of responses made by the United States and Europe.

Corporate information security

In addition to the government, it is also urgently necessary for businesses and universities to improve technology controls.

Businesses and universities across the United States are working to voluntarily step up controls through management initiatives that go beyond complying with statutory requirements from the perspective of sensitive technology control. They require research partner organizations to build similar robust control systems in order to prevent sensitive technology from leaking to an outside party.

For Japanese companies, keeping a technological competitive advantage is necessary, but this goal is not achievable alone, without cooperating internationally with their counterparts in the United States and Europe. Businesses in Japan must stay flexible to respond to unfolding developments in this regard.

In Japan, there are a number of cases in which a single company is engaged in more than one joint research project with scientists at American universities separately from those with Chinese tech companies. Firewalls to ensure network security are critically important in this context to prevent sensitive intelligence from leaking to China within the same organization. Japanese suppliers must realize that they run the risk of losing partnerships or business with American universities or client companies without a firewall in place.

The same holds true for universities in Japan. A growing number of colleges and universities across Japan have accepted researchers and students from China in recent years. It is understandable that those universities in need of research funding are attracted by joint research projects with Chinese colleges and businesses with abundant funding. This dangerous attraction is a pitfall for Japanese businesses. With few exceptions, many businesses lured by abundant

Chinese research funding have little sense of the danger and naïve security management, making it easy for China to steal sensitive technologies. If this situation remains unaddressed, Japan runs the risk of being excluded from the US list of partners for joint research activities.

Businesses and universities in Japan must realize that they operate without having a specific in-house information security system in place, particularly in the area of cyber security.

It is critical for businesses to introduce a security clearance system checking the statuses granting certain individuals access to sensitive technologies. This system is in place in businesses with more than 100,000 employees in the United States.

It looks possible that American businesses will begin suspending initiatives to share sensitive business information with their partners in Japan if they fail to comply with security clearance requirements without a specific system in place that appears reliable to the United States.

It is also urgently necessary for Japanese businesses to stay prepared for cyber-attacks. Many businesses with a tremendous amount of sensitive technology information are still unprepared for cyber-attacks. The US government remains extremely nervous about China's industrial espionage which is aimed at using cyber-attacks to gather sensitive technological information.

China has announced a "self-developed" jet engine C919 in an effort to catch up quickly with Boeing and Airbus in the field of large-sized commercial jets. However, development of the engine was made possible by cyber-attacks targeting component manufacturers in the United States and France. In other words, China has copied engines originally developed by US-France joint venture companies.

In recent shocking news, Mitsubishi Electric, a key player in Japan's defense industry, was targeted by a Chinese hacking group related to the Chinese army. It is also shocking to know that many business leaders in Japan remain indifferent in the face of very real cyber-attacks. A number of companies in Japan are still without in-house cyber security experts to analyze the risks associated with cyber-attacks.

The US government requires many businesses, beyond just defense procurement, to practice strict compliance with administrative guidelines, extending even to extensive groups of players indirectly involved in business transactions. It is even possible that foreign businesses may be cut out of the US supply chain if they fail to comply with government guidelines.

Japanese companies with weak security awareness

With the economy closely linked to national security interests, business leaders in Japan must maintain a keen awareness of security, regard the US-China dispute as a business risk affecting their companies, and not stay on the sidelines.

It is also important for them to establish an in-house security system because the existing export control system is no longer capable of handling the growing business risks surrounding the companies. It will be necessary to establish an integrated security system within the organization reporting directly to the executive team without having subordinate divisions independently responsible for export controls, R&D and information systems tasks.

It will be quite important to national security interests for the Japanese companies doing business with both American and Chinese companies to identify sensitive technologies. Japanese businesses will be required to stay extra careful about key industrial sectors such as artificial intelligence, quantum technology, 5G mobile telecommunications, and video surveillance technology while watching the moves of the United States. Japan must not fall into the same trap Toshiba fell into in the CoCom violation scandal. Japanese business leaders must realize that the disruption of a supply chain in certain specific areas will pose a significant business risk.

Furthermore, it will not be enough for Japanese businesses to only continue statutory checks when trying to comply with the US regulations. If you try to reap benefits from the US-China dispute, you may be subject to sanctions imposed by the United States for serving the interest of an adversary even if it does not breach regulations. Japanese business leaders must realize that they should stay extra careful when doing business with companies on the Entity List.

Meanwhile, certain Japanese companies have been shocked to realize that their data from a joint research project with a Chinese partner company is subject to permission from the Chinese government before being exported to Japan, despite initial happiness after the research project agreement was concluded.

China is fully engaged in efforts to leverage its economic tools to win its battle with the United States. China is set to announce competitive systems and regulations in rapid succession, such as export control regulations and China's own entity list.

On January 1, 2020, China enacted a law to regulate cryptography. There is a growing concern among foreign companies doing business in China that the new law will undermine information security. It is important for business leaders to analyze all these developments unfolding between the United States and China as significant risks affecting their business.

Exploring open innovation opportunities in the United States and China

Meanwhile, China has seen remarkable progress in their own technological innovation in recent years. It is also important that we fairly analyze China's recent innovative success.

The Chinese government actively pours money into scientific research, luring excellent researchers from abroad. China is seeing the rapid development of its innovation ecosystems, driven by abundant research funding from the government. China challenges the United States for the top government in the world in terms of R&D spending and the number of research scientists. Accordingly, there has been rapid growth in the number of published academic articles and patent applications in China. China looks as if it has become entirely a special economic zone, and the pace of its social implementation is astonishing.

Given this situation, Japanese companies have been facing a severe competitive environment in which the existing business model merely relying on their own technological development efforts no longer provides assurances of future business growth. It is here that open innovation comes into play as a primary tool for Japanese companies to boost their competitive edge. Therefore, it is also important that Japanese companies work closely with not only the United

States but also China, a state with huge markets and significant potential for innovation.

To protect its own security interests, Japan must step up its efforts regarding risk management and technological controls. This is the new challenge confronting Japanese businesses in the wake of the US-China tech battle. Japanese businesses are being tested by this new challenge to their future growth.

Translated from "Kigyo mo daigaku mo 'Kibi Gijutsu' no Kanri wo Isoge: Bei-Chu gijutsu haken de towareru 'akusesu tengoku Nippon' no taio (Industry and academia must hurry to step up their control of sensitive technologies: How Japan should avoid becoming a loophole for technology leaks to China in the US-China technology war)," Chuokoron, *March 2020, pp. 118-125. (Courtesy of Chuo Koron Shinsha)* [March 2020]

HOSOKAWA Masahiko
Professor, Chubu University

Born 1955. Graduated from the University of Tokyo with a degree in Law and joined the Japanese Ministry of International Trade and Industry (present-day Ministry of Economy, Trade and Industry).
Served as Director, Americas Division, International Trade Policy Bureau; Director, Security Export Control Division, International Trade Administration Bureau. Visiting Scholar, Stanford University; Harvard Business School AMP. As Director-General, Chubu Bureau of Economy Trade and Industry, advocated Greater Nagoya Initiative. Serving in the current position since 2009. He appears on TV as a commentator. His publications include "*Mega rijon no kobo* (The Battle of the Mega-Regions)" and "*Boso Toranpu to dokusai no Shukinpei ni dou tachimukauka?* (How do we deal with the Uncontrollable Donald Trump and Dictator Xi Jinping?)"
Serving in his current position since 2009, Professor Hosokawa specializes in Japanese and global economics.
