What Is “Economic Security”?

Kitamura Shigeru, former Secretary General of the National Security Secretariat, delves into specific areas of contention in the field of “economic security” both internationally and domestically and considers the future direction of economic security policy in Japan.


Mr. Kitamura Shigeru

On July 7, 2020, I retired from the post of Secretary General of the National Security Secretariat (NSS), following a career in the civil service spanning forty-one years. That career began in 1980, when I joined the National Police Agency (NPA), the last nine-and-a-half years of which were spent in the Prime Minister’s Office.

On the occasion of my retirement from government service, my good friend and longest-serving Director of National Intelligence James Clapper told me, “As you know, we can’t stay in these positions indefinitely.” I agree wholeheartedly – you have to quit sometime. You can only do the work for so long, and in December I will turn sixty-five years old. The French term *ça suffit* may be putting a bit strong, but I have certainly had enough (laugh).

As has been reported already, my focus has been on having surgery for osteoarthritis of the right hip joint and my recovery following my retirement. Since the beginning of 2021, I have been experiencing severe pain and cannot get through the night without pain relief medication.

I was appointed Secretary General of NSS in September 2019 and was primarily in charge of diplomatic and security policies. That period saw regime transitions and regime changes, from the Abe administration to the Suga administration in Japan and the Trump administration to the Biden administration in the United States. During this period of administration transitions, our focus was on maintaining and deepening the Japan-US alliance. Much attention was directed to negotiations with the US’s National Security Council (NSC). We could keep the continuity of security policies between Japan and the United States and unify our goals. One of the major tasks I handled in the NSS was the establishment in April 2020 of an “economic division“ to promote economic security policies. The economic section is the control tower of “security in the economic field” and is responsible for policy planning and overall coordination. It is an impressive organization comprising a total of twenty highly skilled and experienced members (as of July 11, 2021) under the Cabinet Secretariat Fujii Toshihiko from the Ministry of Economy, Trade, and Industry, with four Councillors dispatched from the Ministry of Finance, Ministry of Internal Affairs, Ministry of Foreign Affairs, and the NPA.

Illegal Exports of Advanced Technologies

The world is entering an era of “economic security.” The word “security” tends to evoke military associations. However, the field of security has been expanding in recent years into the economy.

Whereas the past saw military technologies such as the Internet diverted to use by the private sector, now advanced technologies from the private sector such as AI and drones are being diverted to military use, resulting in a shift in the industrial structure. China is also strengthening its hegemony, bolstering its military power by advancing its “Civil-Military Integration” policy that integrates the military and private sectors.
In my role as a police bureaucrat, I have been in the foreign affairs field for a long time and have handled many cases of violations of the Foreign Exchange and Foreign Trade Act (FECA). This has enabled me to witness the easy outflow of Japan’s advanced technologies to other countries. One such instance is the unauthorized export of unmanned helicopters to China by Yamaha Motor.

In February 2007, the Shizuoka and Fukuoka Prefectural Police arrested executives of Yamaha Motor on suspicion of attempting to export unmanned helicopters used for pesticide spraying and aerial photography to an aerial photography company in Beijing, China. Unmanned helicopters can be diverted for military purposes, and their export is regulated under the Foreign Exchange Act. However, Yamaha Motor deliberately under-declared their capabilities and continued exporting them without authorization to China. Given that the export destination is closely linked to the People’s Liberation Army (PLA), it is likely that the unmanned helicopters were diverted to military use.

It is becoming a thing of the past for foreign intelligence agencies to obtain classified military and political information. Intelligence agencies around the world now target advanced technologies owned by governments and companies.

The economic division of the NSS was established out of a sense of crisis about these changed global circumstances. Japan is no exception for issues that have arisen in areas that cut across security and economy. As will be discussed later, these include investment by the major Chinese IT company Tencent in the Japanese e-commerce company Rakuten Group, restrictions on foreign ownership and shareholders’ voting rights in Toshiba, the case of personal data of Line users, and the relationship between the Science Council of Japan (SCJ) and China’s Thousand Talents Plan. Many issues behind the news and companies that are household names are about economic security.

Despite this, no genuine shared concept of “economic security” exists in Japan beyond specific political and bureaucratic organizations, nor is there a sense of mounting crisis. As the person responsible for setting up the economic division of the NSS, I accepted this interview to explain what is happening in the world right now and what kind of system is needed in Japan.

Three Aspects of Economic Security

While no clear definition of economic security exists, three major aspects can be identified.
One is a concept termed “economic statecraft,” which refers to the pursuit of national interests by applying economic measures to diplomacy and security. The most obvious example is economic sanctions. In 2010, when the Democratic Party of Japan (DPJ) was in power, China halted the export of rare earth elements to Japan in protest against the Japanese government’s detention of the captain of a Chinese fishing boat involved in a collision incident off the Senkaku Islands. As a result, the price of rare earth elements soared, forcing Japanese companies to bear the burden. This can be seen as an “attack” on other countries through economic measures. The second is the defensive aspect, which refers to the protection of Japan’s technologies. As mentioned earlier, there is currently an outflow of advanced technologies owned by Japanese companies to other countries. Those technologies may include human resources, as in the case of Japanese companies being acquired by foreign companies. Laws and regulations such as the Foreign Exchange Act have become essential mechanisms to guard against such a scenario. The third aspect is the maintenance of a “free and open international economic system.” This requires countries to form economic partnerships based on shared values such as the rule of law, free and fair trade, and democracy. International regulations that accord with these values through frameworks such as QUAD between Japan, the United States, Australia, and India will need to be formulated.

“Data Is the Nation”

What, then, is the most critical aspect of economic security? The first thing to keep in mind is that the twenty-first century is the “data age.”

At the Davos meeting (World Economic Forum Annual Meeting) in January 2019, former Prime Minister Abe Shinzo made the following speech.

“It took three to four decades before we humans came to know the value of gasoline. About twenty years into the twentieth century, gasoline was running cars and flying airplanes.
“It is the same, isn’t it, about data. Around 1995, we started to use the Internet on a massive scale, but it was almost twenty years into the twenty-first century that we found data driving our economy.”

In the twentieth century, oil made the world go round. The oil fields that hold oil reserves, the pipelines through which oil is transported, the refineries where crude oil is refined, and steel as the backbone behind it all. The nation that controlled every part of this process became the supreme global power.

However, the oil age is drawing close, and we are already moving into the data age. The global superpower will be the nation that controls data. A fierce rivalry has begun over technological hegemony over data, and “data is the nation” has replaced “iron is the nation.”
From now on, the totality of technologies that handle data will determine the fate of our country: data centers to store data, submarine cables and 5G to transmit data, Beyond 5G technology, AI and quantum computing technology for data analysis, and manufacturing technology for semiconductors used in smartphones and all other types of devices. This is why economic security policies are urgently needed to deal with the rivalry over technological hegemony in the data age.

What Has China Set Its Sights On?

We need hardly say that China’s economic and military rise triggered a heightened awareness of the economic security crisis. Since the 1990s, China has been expanding its military and economic power by taking advantage of its vast land and population size, backed by the political power of its one-party regime.

In recent years, however, it has become clear that a vast gap exists between the concept of “international order” espoused by developed countries of the West and that of China. The international order that Western developed countries are aiming to achieve is, as mentioned earlier, a “free, open, rules-based world,” in which each country is equal and works together based on shared values that respect the rule of law, freedom, and equality. What, then, is the “international order” that China is aiming to achieve? President Xi Jinping often uses a “new type of international relations,” which ultimately challenges the current “international order.” For a long time, China has been investing heavily in infrastructure development in developing countries in Asia and Africa under the Belt and Road Initiative (BRI), a vast economic zone concept. The ultimate goal is to create a framework through an informal alliance with Chinese financial backing. Moreover, China aims not to create an equal relationship but a pyramid-shaped association of nations with China at the top based on Sinocentrism.

Until now, Western countries have been competing with China for technological hegemony based on the assumption that they are fighting for first and second place in pursuit of the same goal. That assumption was false, and it is becoming increasingly clear that the contest is not about technology alone. Instead, President Xi Jinping has set his sights on a future entirely different from the one we envisage.

The United States was quick to notice China’s political ambition and change tack. This was exemplified by the following comment made by my counterpart in the Trump administration, National Security Advisor Robert C. O’Brien, in a speech on June 24, 2020: “The days of American passivity and naivety regarding the People’s Republic of China are over.”

There followed a succession of speeches by the president's aides criticizing China, by Christopher Wray, Director of the Federal Bureau of Investigation (FBI) on July 7 of the same year, then United States Attorney General William Barr on July 16, and then-Secretary of State Mike Pompeo on July 23.

Preventing the Outflow of Advanced Technologies

Looking back at the history of US-China relations, the United States has pursued a policy of engagement with China since the establishment of diplomatic ties in 1979. In the Cold War between the United States and the Soviet Union, the core of its strategic thinking was likely to have been the desire to use China as a counterbalance to contain the Soviet Union.

During the same period, the introduction of the "[socialist] market economy" that set forth Deng Xiaoping's Reform and Opening-up economic policy was also significant. It led the United States to believe that China was on a path to democracy because it wished to be like the US and that maintaining a connection would bring them full cooperation.

However, the rise of China has revealed differences in the political system and thought, exemplified by the human rights issue in the Xinjiang Uygur Autonomous Region and the hardline stance toward Hong Kong, leading the United States to change its policy. The so-called blind engagement policy pursued by the Nixon administration through to the Obama administration was finally abandoned by the Trump administration.

On the other hand, even while continuing its engagement policy, the United States remains locked in intense competition with China over technological hegemony. In March 2012, Ralls Corporation in Delaware, which was owned by two Chinese nationals, acquired four wind power companies in Oregon to cite a real-life example. In July of the same year, the Committee on Foreign Investment in the United States (CFIUS) issued an interim order to Ralls Corporation requesting that it cease construction and operations at the project site and prohibit access to the site. The order was issued because Ralls Corporation's planned wind power generation business was in an air defense restricted area controlled by the US Navy in Oregon. In a presidential decree issued in September of the same year, then President Obama said, "There is credible evidence that leads me to believe" that Ralls Corporation and other persons concerned "might take action that threatens to impair the national security of the United States."

The Trump administration's increasingly hardline stance toward China led to a further review of those regulatory systems to prevent the outflow of advanced technologies. The core of the study was the "tightening of [foreign] investment controls" and the "tightening of export controls."

To address the tightening of investment controls, on August 13, 2018, the Foreign Investment Risk Review Modernization Act (FIRRMA) was enacted to strengthen the CFIUS. The CFIUS is the

committee that reviews foreign investment in the United States. The points of the amendment expanded the authority of the CFIUS by, for example, expanding the scope of its review and allowing the committee to share information with allies. The Export Control Reform Act (ECRA) was passed at the same time. Work is currently underway to identify target technologies to tighten export control of emerging and foundational technologies such as AI and quantum technology.

These examples of ex post facto intervention by public authorities to strengthen regulatory systems will serve as a reference for Japan when designing its plans in the future.

The loophole in the Revised Foreign Exchange Act

Japan, too, is facing many problems related to economic security.
In March 2020, the Rakuten Group announced a capital tie-up with major Chinese IT company Tencent. Tencent invested approximately 65.7 billion yen in Rakuten, becoming the majority shareholder with a 3.65% stake. Unfortunately, I first learned about the tie-up from the front page of *The Nikkei* on March 13. I recall being concerned and calling the person in charge of the economic division.

The Revised Foreign Exchange Act, enacted in May last year to tighten restrictions on foreign investment, lowered the investment ratio threshold subject to prior notification when foreign investors seek to invest in core companies in business sectors that may impact Japan's national security from 10% to 1%.

Tencent's investment in Rakuten was 3.65%, yet no prior notification was filed. The Revised Foreign Exchange Act exempts companies from filing a prior notice if they meet specific "exemption criteria," such as not accessing undisclosed critical technologies and "additional criteria," such as not participating in board meetings. Tencent explained that the purpose of the investment was to make a "net investment" that does not entail involvement in the company's management. Hence, it was able to invest without filing a prior notification.
A capital tie-up with a Chinese company inevitably poses certain economic security risks. CEO & Chairman of the Rakuten Group Mikitani Hiroshi explained that through this capital tie-up, "Tencent will have no involvement whatsoever in the management of Rakuten." This statement may satisfy the Japanese authorities, but how about the US? Naturally, the US authorities are watching this case closely. There will be ongoing ex-post monitoring to ensure that Tencent complies with the exemption criteria and that Rakuten's sensitive information is not being leaked to China.

Further, Rakuten's US business needs to be watched closely. In 2020, the US government selected Rakuten Mobile for its 5G Clean Network, so Rakuten is now operating in the US 5G Clean Network, a mechanism to keep telecommunications services in the US safe from China, with access restricted to trusted operators only. While this is only a policy framework of the former Trump administration, it may raise awareness of the issue from the US side.

Shareholder Rights or Investment Regulation?

In the battle between Toshiba and the foreign investment fund, the economic security perspective seems to have been overlooked.

An investigative report released on June 10, 2021, by external lawyers appointed by the Singapore investment fund and Toshiba's top shareholder Effissimo Capital Management caused a stir. The investigation sought to determine whether or not the annual shareholders meeting held on July 31, 2020, was conducted fairly. Effissimo proposed its plan for board appointments for its upcoming annual shareholders' meeting in July 2020. The report said that Toshiba and the Ministry of Economic, Trade, and Industry (METI) colluded to pressure Effissimo to refrain from exercising its shareholder's right of proposal and voting request. It also noted that detailed e-mail exchanges between senior officials of METI and board members of Toshiba revealed "undue pressure on shareholders." This report led to a great deal of media criticism of Toshiba and METI.

The media's sole focus on the rights of shareholders is, however, one-sided. Toshiba is involved in the nuclear power and quantum cryptography businesses, closely related to Japan's security. From a security perspective, it is not illegal for Toshiba to provide information to METI and for METI to offer the appropriate advice, and it is par for the course. Whether Japan prioritizes the exercise of minority shareholders' interests or investment regulation under the Foreign Exchange Act will be a significant issue in the future as it bolsters its economic security. Either way, more stringent procedures will be required for foreign investors to acquire shares in core companies dealing in advanced technologies.

A further issue is the viewing of personal information on the accessible communication app "LINE." In April 2021, a report by the *Asahi Shimbun* revealed that the personal information of some LINE users is being stored in a data center in South Korea. It was also discovered that LINE had outsourced its operations to Chinese companies and that users' personal information could be viewed from China. LINE was initially started by the Japanese subsidiary of Korean IT giant Naver. After merging with Yahoo Japan Corporation's parent company Z Holdings, outsourcing operations to Korea and China in March this year was highly predictable.

The LINE issue has brought to the fore the question of where to store data. Until now, the trend among Japanese companies has been to prioritize cost considerations, believing that data can be placed in any country. As a result, data has often been stored overseas. However, in 2017, China enacted the National Intelligence Law, which requires private companies to cooperate with state intelligence gathering. Given that there is a high risk of information stored in China being reported to the National Security Bureau, this involves the issue of security.

Since the problem came to light, LINE has been completely blocking access from China and moving all of its servers into Japan. From a security perspective, dependence on data centers in other countries is not always desirable. In the future, other Japanese companies will be required to do the same.

Transfer of Invisible Technology

The domain of economic security is not limited to corporations but extends to universities and research institutions. This is because some of the technologies being researched at universities are closely related to security.

In September 2020, the Science Council of Japan (SCJ) was in the spotlight due to the issue of the refusal of the Prime Minister to appoint members. At the same time, the relationship between the SCJ and China's "Thousand Talents Plan" was brought into focus. The Thousand Talents Plan is a national project launched by the Chinese government in 2008 to bring outstanding researchers from various countries to China. SCJ officials are said to have been involved in this project. Moreover, they are said to have been affiliated with the "Seven Sons of National Defence (Seven Sons)." Seven Sons is the umbrella term for universities such as Beijing Aeronautics and Astronautics University, Beijing Institute of Technology, and Harbin Institute of Technology, under the Ministry of Industry and Information Technology (MIT), which integrates the military and defense industry. The Seven Sons were established to provide human resources to the PLA and the military sector as part of China's "civil-military integration" strategy. In other words, there are concerns that the research conducted here could be diverted for military purposes. In 2017, the SCJ issued a Statement on Research for Military Security in which it declared that Japan's universities and other research institutions would not conduct scientific research for military purposes. Nevertheless, it has left itself open to accusations of operating under a "double standard."

Other Japanese researchers are also said to be enrolled at the Seven Sons due to academic exchange agreements concluded between the Seven Sons and several leading universities in Japan. Some of those researchers would appear to have been awarded the highest degrees in science and technology in China. This has led to an outflow of knowledge possessed by Japanese researchers through academic exchanges and personnel exchanges, a situation known as "Intangible Technology Transfer." Already, the United States is stepping up measures to counteract this situation. FBI Director Christopher Wray claims that China uses its researchers and exchange students to gather US intellectual property and has been tightening its approach regarding Chinese students. There was even a move to revoke international students' visas believed to be associated with the PLA.

Japan, too, will need to thoroughly investigate students and researchers entering the country from overseas to determine their background. With the United States becoming increasingly wary of China, Japan may be excluded from the global research network if it continues its current practices.

Identification of Technology, Development of Technology, and Preservation of Technology

A further issue is the future direction of economic security policy in Japan. On June 18, 2021, the government decided on the Basic Policy on Economic and Fiscal Management and Reform 2021 and the Action Plan for Growth Strategy related to the fundamental principle of economic security. The latter, in particular, may be considered an outcome of the Japanese government's economic security policy at present. In a nutshell, it states that “identification” of technology, “development” of technology, and “preservation” of technology will be critical for Japan to secure technological superiority in a future of economic security.

The first step is to “identify” which of the technologies Japan possesses are essential for security. This requires the creation of a mechanism for relevant ministries and agencies to collaborate in the selection of technologies to be developed and preserved.

Next is the “development” of key technologies. The government must support key advanced technologies in space, quantum, AI, supercomputers, semiconductors, nuclear power, advanced materials, biotechnology, and oceans.

Semiconductors, in particular, have seen a particularly dramatic decline in Japan. The sales share of semiconductors for Japanese companies fell from 50.3% in 1988 to 10.0% in 2019. Investments are the most effective way to develop businesses. In the case of semiconductors, however, it takes trillions to build a new factory. China is making a significant investment of more than 5 trillion yen in semiconductor technologies, quite a different order of magnitude from that of Japan: METI's budget for subsidies and other assistance is in the tens of billions of yen range at the most. Japan needs to undertake special initiatives, such as setting up a semiconductor plant in a joint venture with a significant overseas contract manufacturer.

Finally, how should the technologies that have been identified and developed be “preserved”? As mentioned earlier, there is a need to review export controls and vet inward direct investments more thoroughly. This can be handled through the current system for the time being, but legal changes may become necessary in certain areas at some point.

Can We Gain Public Understanding?

The critical question is whether Japan can gain the understanding of the public. There is a need to raise awareness of economic security through proactive public relations and educational activities.

In a sense, the economic security policy may be regarded as a regulatory policy since state intervention often occurs. This can be easily misinterpreted as “state coercion” or “inhibiting free competition,” as

happened with the Toshiba issue. Such accusations will constitute weapons in the arsenal of opponents. However, these economic security policies aim to promote free and fair competition by correcting injustices on the part of foreign countries and companies. Ultimately, the nation and its people will benefit. It is my sincere hope that this article will help firmly cement public awareness of such issues.

Translated from" 'Keizai Anzenhosho' towa Nanika?—Toshiba jiken, Gakujutsukai mondai nadono shinso wo zen Kokka anzenhosho kyokucho ga kataritsukusu (What Is "Economic Security"?— The former Secretary General of the National Security Secretariat delves into the Toshiba issue, academic issues, and other areas of contention)," Bungeishunju, September 2021, pp. 144-155. (Courtesy of Bungeishunju, Ltd.)

KITAMURA Shigeru is the former Secretary General of the National Security Secretariat and president of Kitamura Economic Security Inc.