YOUNG LEADERS PROGRAM

GIVING OLD SPY-HUNTERS A NEW JOB – COUNTERING ECONOMIC ESPIONAGE

BY REI KOGA

Rei Koga *is a Ph.D. candidate in International Political Economy at the Department of European and International Studies, King's College London (KCL). Her research interest revolves around Chinese economic statecraft and responses in the Indo-Pacific region. Prior to joining King's, she studied at the University of Bristol and was awarded Master of Research in Global Political Economy with Distinction in 2022. During her master's study, she was a Rotary Global Grants Scholarship student. Prior to that, she worked for the Cabinet Secretariat of Japan.*

View of the Ministry of Justice and PSIA. Source: Courtesy of PIXTA

In the past decade, the concept of economic security has grown from a low-key political idea to an integral part of contemporary national security. During the 2023 G7 meeting at Hiroshima, the G7 Leaders' Statement on Economic Resilience and Economic Security showcased this fact by highlighting the importance of mutually beneficial cooperation in this area. The concept covers a wide policy field including energy security, resilience of supply chain, and countering weaponization of economic tools; the precise definition and boundary of economic security is different depending on the state. In this sense, it could be said that the importance of the statement at Hiroshima lies in its step towards standardizing the concept of economic security between like-minded states.

The overarching concept of economic security aspires to protect national security by treating the economic sphere as a relevant part of national security policy considerations, be it critical minerals, foreign direct investment, or dual-use technologies. Some fields are more challenging to regulate than others, none more so than restrictions on dual-use technology. Such technology is by its definition, used both in private and military applications, adding complexity to its regulatory framework. Moreover, sensitive information in need of protection is often originally the creation and property of private enterprises, which may not share the same level of awareness and protection against espionage as the government.

This problem of dual-use technology regulation is especially acute in Japan, where it not only lacks a centralized agency dedicated to counter industrial espionage, but also has a public sentiment environment that is hostile to such institutions. With both traditional and non-traditional industrial espionage on the rise, it is obvious that Japan needs to enhance its intelligence capability to counter such threats. While there are several existing agencies which are involved in similar roles, the Public Security Intelligence Agency (PSIA) seems to be the most suitable one and its capabilities need to be reinforced.

Why PSIA?

While there are several Japanese government agencies that have dealt with counter-industrial espionage before such as the National Police Agency (NPA) and the Economic Unit of the National Security Secretariat (NSS), the most suitable agency for that purpose would be the PSIA. If we look at the NSS and its Economic Unit, it has its main mandate set as to coordinate government security policy and is not necessarily expected to execute individual operations and policies. NSS is also operated by government

officials from various agencies, which means there are a limited number of in-house officials who can continue to work in the NSS for long periods of time, reducing its efficiency as an enforcement agency and could be an obstacle to accumulating know-how on the operation of counter-industrial espionage. As for the NPA, while it has the capability and manpower for the role, law enforcement and intelligence gathering need to be separated for fear of becoming a police state. Not only does this process of elimination shed light on the suitability of PSIA as the chief operating body for counter-industrial espionage, but there are also features which make it suitable for the job. The following section will discuss this point as well as policy suggestions to enhance its capabilities.

The PSIA was established in 1952 and is responsible for protecting Japan's public security, with its mandate set under the Subversive Activities Prevention Act and the Act on the Control of Organizations. Its focus was originally centered around anti-left-wing rioters, which gradually evolved to include counterterrorism in the 1990s, but now it recognizes itself as an agency which also engages in collecting information on economic security. This shift seems to be in accordance with the trend of security threats surrounding Japan. To accelerate these efforts, this paper suggests revising the foundation law of PSIA.

As of February 2024, although the PSIA continues to seek to enhance its role in the field of counter-industrial espionage, its mandate is insufficient because its foundation law has not been revised according to the role it seeks to play, with its jurisdiction unchanged since the introduction of the Act on the Control of Organizations of 1999. While building up de facto capability is important, the PSIA's legal mandate is also essential in several ways. Firstly, the legal mandate enables the PSIA to conduct the Plan–Do–Check–Act cycle, leading to a systemized self-evaluation of its operations. As intelligence operations are by nature mostly inaccessible to outside regulation, securing such a mechanism is essential. Secondly, the PSIA operates with the mandate of the Subversive Activities Prevention Act, which does not perfectly suit the nature of counter industrial espionage. The act came into effect in 1952 and aims to prescribe necessary control measures on an organization which has conducted a terroristic subversive activity as an organizational activity, and has supplemented penalties for terroristic subversive activities, thereby contributing to ensuring public security. One of the limitations set by the act towards the PSIA is that it can only monitor and restrict organizational targets. Industrial espionage is not always conducted at an organizational level and individuals are better at concealing their affiliations. This means that the act which designates organizational entities as the target for the PSIA's surveillance and restriction is not adequate in dealing with industrial espionage. Therefore, it is necessary to give the PSIA a mandate, preferably a separate economic security-related law to include such individual-level activities. Thirdly, information sharing inside the government needs to be systemized. While the information gathered by the PSIA is important, it also needs to be shared with the policy-making side as well. For instance, the PSIA's counter-espionage intelligence can be used for national security assessments by the Ministry of Finance and other relevant ministries when assessing foreign direct investment cases, which is said to be one of the main routes for sensitive technology leakage. If such a scheme is not written in law and relies on customs and practices, the legality of information sharing will be unstable, therefore institutionalizing such inter-agency intelligence-sharing cooperation is important.

Long-Term Effect of Building Up Capability

Reinforcing the PSIA will bring several benefits to Japanese economic security agendas. Firstly, with a more dedicated mandate for the PSIA, cooperation and trust-building with like-minded countries in the counter-industrial espionage field will be facilitated. It has long been pointed out that Japan is lacking in its counter-espionage capabilities, creating obstacles for international information sharing and joint R&D with other states. If Japan can gain the trust of its like-minded countries through the reinforcement of the PSIA, its situation and reputation will be improved, leading to more opportunities for intelligence-sharing.

According to a survey report by KPMG and Thomson Reuters, 7.2% of the companies surveyed answered that they established a specialized team dedicated to economic security, while around 44% answered that they have existing groups in charge of it. This means around 40% of companies have not taken any measures to get themselves ready to defend themselves against economic espionage. Within these divergent responses, around 56% of them listed information evaluation and risk assessment as one of their challenges in relation to economic security. This altogether means that a majority of Japanese companies require assistance in some form to operate in accordance with the changing legislation. Fortunately, the PSIA has regional branches across Japan. While such regional offices have long served as information-gathering branches for counterterrorism, they could form a basis for close communication and advice for the business sides as well, although it may take time to foster a proper relationship between the two sides due to the image of the PSIA as a counterterrorism agency.

Challenges Ahead

The above policy change recommendations are likely to encounter some obstacles. Probably the most significant one will be related to whether the Japanese society/politics are open to discussing such reinforcement of intelligence capacity. In general, the Japanese population has a significantly lower tolerance against the state strengthening public security compared to many other Western industrialized countries, partly due to the memories of the state using the Special Higher Police and military police to suppress freedom of speech before and during the Second World War. A good example is the 2013 debate on the Act on the Protection of Specially Designated Secrets, in which the government faced unprecedented public opposition. The Japanese public and the opposition party focused on concerns regarding the people's right to know, and very little time was allocated towards debating the specific types and nature of the intelligence that was the object of protection under the Act. However, there has already been a case in which economic security breach investigations have led to false accusations (the case with DeRight Precision Machinery Co.,Ltd., also known as Ohkawara Kakohki Company). In an ironic twist of fate, the failure of the police in handling this case may actually encourage the government to enhance the capabilities of its intelligence agencies and strengthen coordination with law enforcement to prevent similar cases in the future.

Disclaimer: All opinions in this article are solely those of the author and do not represent any organization.