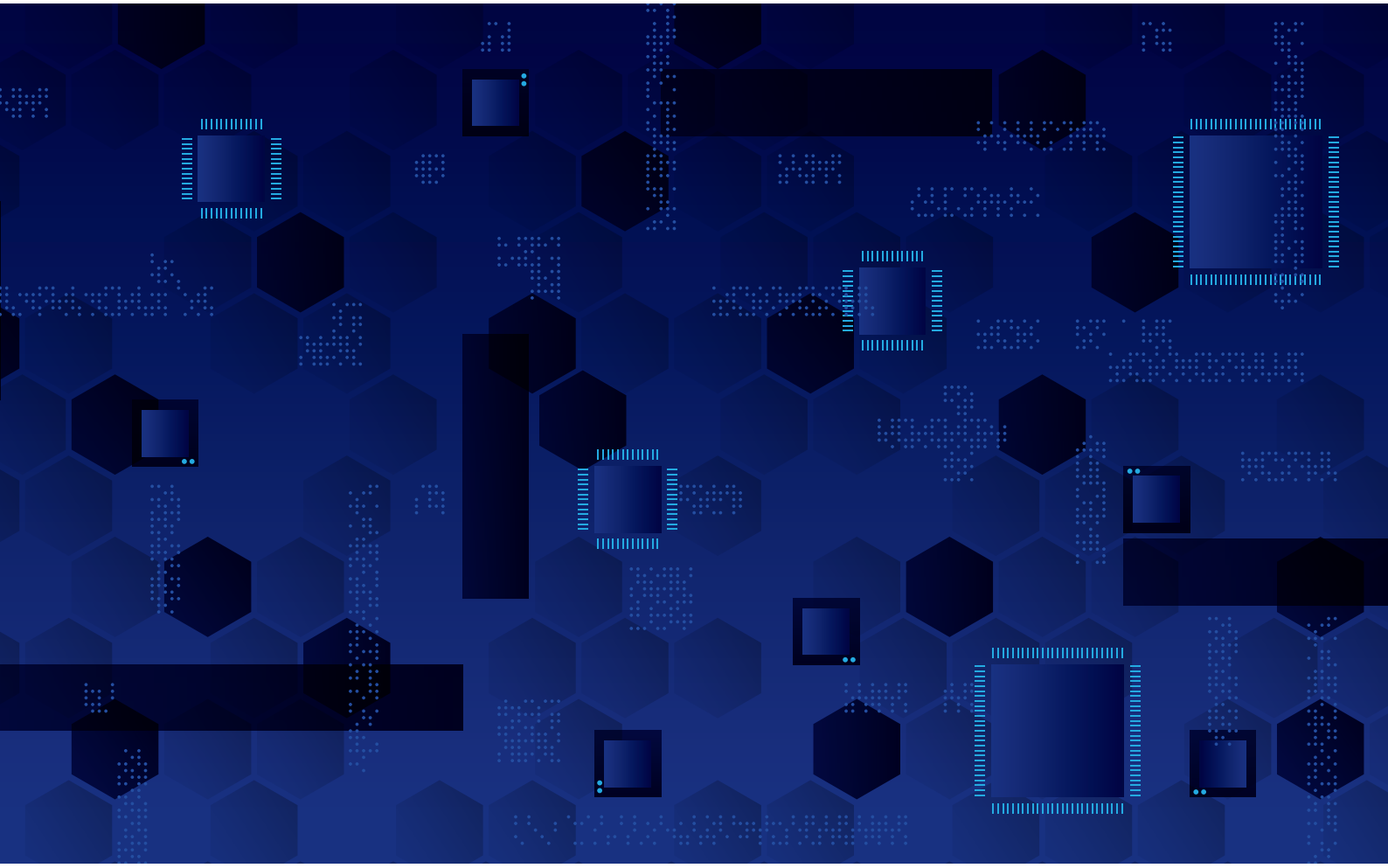
Ensuring Economic Security 2022

Preventing leak of technologies, data, and products



Public Security Intelligence Agency

Introduction

In the international community, currently it has become important to address security issues related to economy and advanced technology. As each country is increasingly seeking to acquire technologies, data, and products to improve its own manufacturing capacity and technologies, there have been cases in Japan as well, such as achieving the purpose by approaching target companies, universities, etc. under the guise of appropriate economic or research activities.

If technologies, data, and products are leaked out of Japan, they may be diverted to research and development and other purposes of weapons of mass destruction, etc., or the technological superiority possessed by Japanese companies, universities and other institutions may be lost, which in turn may threaten the security of the nation and its people, or lead to the loss of international competitiveness. Therefore, it is of utmost importance to prevent the leak of technologies, data, and products by implementing measures to ensure economic security with cooperation between the public and private sectors, based on the proper recognition of such risks.

This pamphlet has been prepared to inform the public about the current situation, which should be kept in mind from the viewpoint of economic security. We hope that it will help your understanding.

Contents

Public Security Intelligence Agency's Efforts

In Japan, in order to maintain peace in our country, and to ensure the safety and security of its people, various initiatives have been promoted to "know" the threats and the technology to respond to them, "develop" the necessary technology, "utilize" the developed technology in social implementation, and "protect" against the leak of such technology.
Among these, in order to contribute to "protection," the Public Security Intelligence Agency, as a member of Japan's intelligence community, in cooperation with relevant organizations, collects and analyzes information on trends of concern targeting technologies, data, and products owned by Japanese companies, universities, etc., and information related to the use of influence through economic activities, and provides intelligence to relevant organizations, including the Prime Minister's Office.

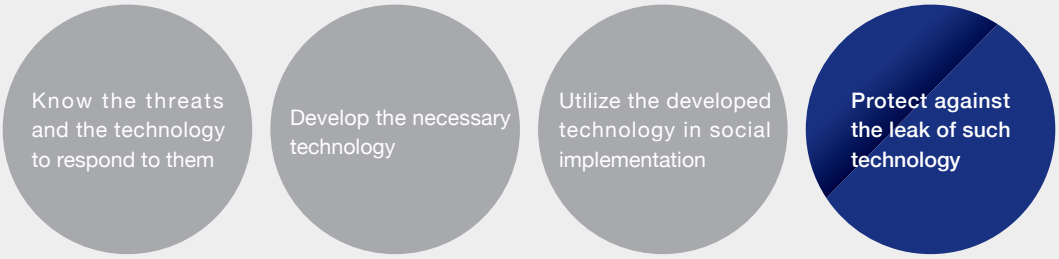
Lecture on economic security given at the Japan Business Federation

Integrated Innovation Strategy 2021

(Cabinet Decision on June 18, 2021)

(Excerpt from the tentative English translation)

"In order to ensure and maintain Japan's technological superiority, the government will ... implement appropriate measures against technology outflow. ... The government will promote information gathering ... in order to take appropriate measures against technology outflow in a phased manner according to the actual situation of various technology outflows, while ... ensuring comprehensive security."



The Public Security Intelligence Agency, as an intelligence agency, collects and analyzes information on such matters as

- trends of concern targeting technologies, data, and products, and
- trends in the use of influence through economic activities by countries of concern.

Contribute to policy making on economic security and prevention of leak of technologies, data, and products

Current Situation Surrounding Japan

The Increasingly Tense US-China Conflict

European Union (EU)

"EU Foreign Direct Investment Screening Regulation" —October 2020

- Screening of foreign direct investment in sensitive technologies and critical infrastructure

New EU industrial strategy "Open Strategic Autonomy" —May 2021

- Identification of products that are highly import-dependent and for which it is difficult to diversify procurement sources or substitute within the region, and strengthening of cooperation in areas of strategic importance

Proposal for an "EU chips act" —February 2022

- Breaking away from dependence on Asian semiconductors, and strengthening research and development, and production in the EU

China

Enactment of "Regulations on the Unreliable Entity List" —September 2020

- Creating lists of foreign organizations and individuals that threaten China's sovereignty, security, and interests, and restriction or prohibition of their import, export, investment, entry into China, etc.

Enactment of "Rules on Counteracting the Unjustified Extraterritorial Application of Foreign Legislations and Order Measures" —January 2021

- Prevention of the application of foreign regulatory laws and regulations in China

Enactment of "Anti-Foreign Sanctions Law" —June 2021

- Allowing for countermeasures at the legal level against "discriminatory restrictive measures" by foreign countries

United Kingdom

"National Security and Investment Act" —January 2022

- Granting the government the authority to scrutinize and intervene in foreign investment, etc.

Germany

Amendment to the "Foreign Trade and Payments Act" —July 2020

- Expanding the scope of notification requirements for investments by non-EU companies

Amendment to the "IT Security Act" —May 2021

- Strengthening of the functions of the Federal Office for Information Security
- Prohibiting the use of components in critical infrastructures if they undermine public safety

France

Amendment to the "Code of Post and Electronic Communications" —August 2019

- Requiring prior examination of telecommunications carriers

Extension of special measures to regulate foreign investment —November 2021

- Extending special measures to protect companies in strategic sectors from acquisition by foreign capital (until the end of December 2022)

Canada

Update to the "Guidelines on the National Security Review of Investments" — March 2021

- Identification of areas that could present national security concerns in foreign investment and review of foreign investment in these areas

Release of "National Security Guidelines for Research Partnerships" — July 2021

- Protection of domestic intellectual property from espionage and other activities

United States of America

Restrictions on entry of Chinese researchers and students — June 2018 onwards

- Stricter visa issuance, etc. for Chinese students, etc. of science and engineering

Posting of Chinese companies on the Entity List based on the "National Defense Authorization Act for 2019" — May 2019 onwards

- Adding many Chinese companies, etc. to the Entity List (list of entities subject to export restrictions) and strengthening export controls to China

(Note: The Entity List includes organizations and individuals involved in activities subject to US sanctions or contrary to the US national security or foreign policy interests. Exports, etc. to those on this list are restricted.)

Exclusion of China from the supply chain of critical technologies and products under the "Executive Order on America's Supply Chains" — February 2021 onwards

- Restrictions on procurement and use of information and telecommunications equipment, etc. made by Chinese companies

Australia

Amendment to the "Foreign Acquisitions and Takeovers Act" — January 2021

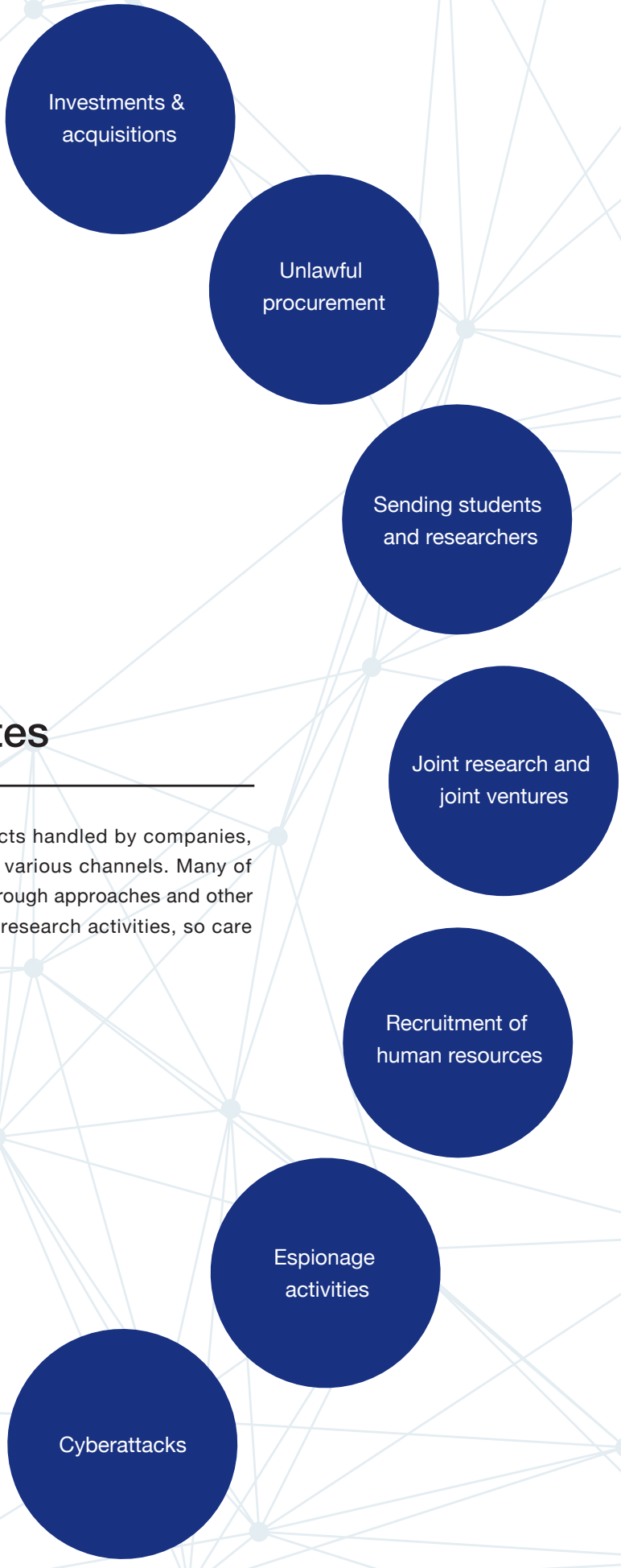
- Mandating government review of foreign investment in land and business sensitive to national security, regardless of the amount of investment

Amendment to the "Security of Critical Infrastructure Act" — December 2021

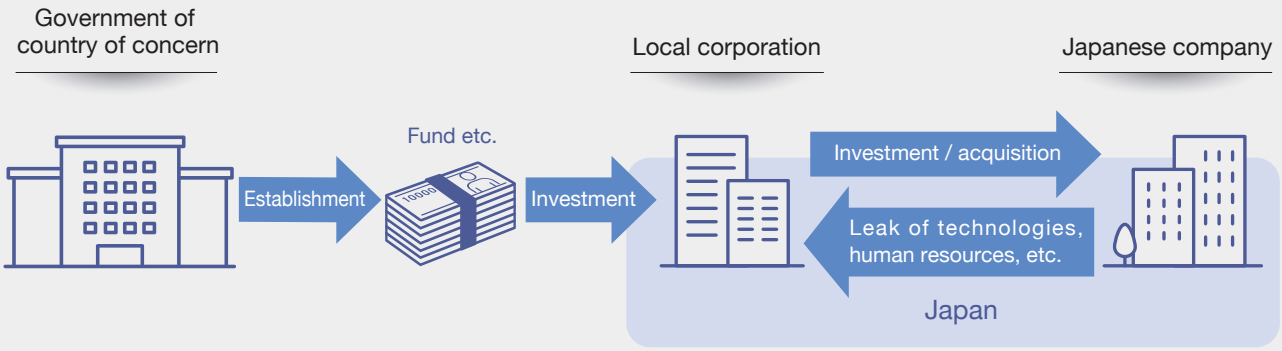
- Expansion of the scope of foreign investment examination from four to 11 sectors

Possible Leak Routes

In Japan, technologies, data, and products handled by companies, universities, etc. may be leaked through various channels. Many of these are believed to have been leaked through approaches and other efforts disguised as proper economic or research activities, so care must be taken.



1 Investments & acquisitions



Cases that actually occurred

Case 1:

A Chinese company planned to establish a subsidiary in Germany in 2020 to acquire a medium-sized telecommunications satellite company in the country. The German authorities blocked the acquisition on the grounds that it could threaten its national security.

Case 2:

A Chinese company planned a series of acquisitions of semiconductor-related companies in South Korea, France, and Taiwan in 2021. According to a Dutch company that analyzes the Chinese economy, the Chinese company in question was effectively under the control of the Chinese government and relocated the research and manufacturing bases of several foreign companies it had acquired thus far to China.

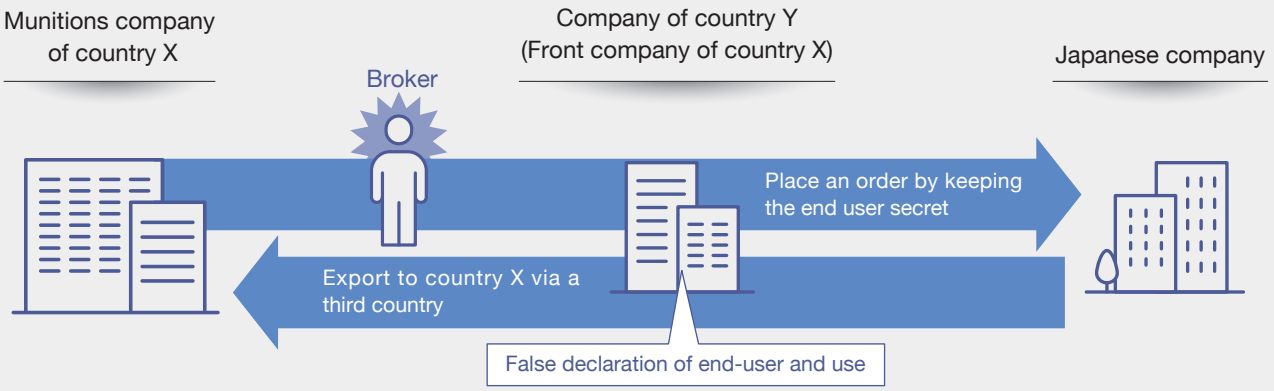
Case 3:

A Chinese company planned to acquire a major Ukrainian aero-engine company in 2021. The US authorities expressed concern about it as a "malicious Chinese investment." The Ukrainian authorities blocked the takeover.

Point

- There is a risk that an investor from a country of concern will acquire a Japanese company that possesses important technologies, resulting in the leak of Japan's technologies, data, and products to the country of concern.
- Even if an investor making the investment or acquisition is not an investor from a country of concern, it may be considered to be substantially under the influence of the country of concern, and the capital relationship should be noted.
- There is a possibility that an investor from a country of concern may seek to acquire companies or acquire highly skilled human resources through newly established corporations, etc. in Japan.

2 Unlawful procurement



Cases that actually occurred

Case 1:

The German authorities announced in 2021 that they had detained A, a person suspected of assisting Russia in the procurement of high-performance machinery. The trading company run by A is believed to have ties to Russian intelligence agencies and to have shipped high-performance machine tools to Russian munitions companies.

Case 2:

In 2018, the US authorities arrested a Chinese national on suspicion of illegally exporting US-made hydrophones (devices used to detect and monitor sound underwater) that could be used in anti-submarine warfare to a Chinese university with close ties to the Chinese People's Liberation Army, based on a request from the university.

Case 3:

In 2021, Iranian national B, a resident of the United Arab Emirates (UAE), was convicted in the United States of illegally exporting US-made parts to Iran that could be used in such systems as nuclear weapons and missile guidance.

Case 4:

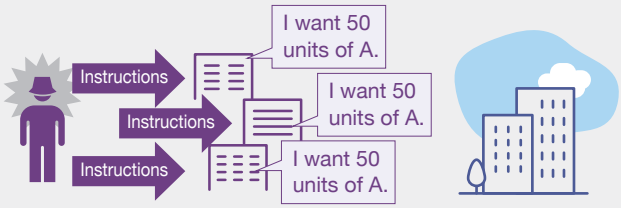
In 2021, the president of a machinery manufacturing company in Japan was referred to the public prosecutor for violation of the Foreign Exchange and Foreign Trade Act (attempted export without obtaining permission) for attempting to export to a Chinese company without obtaining permission a high-performance motor that could be used in military drones.

Point

- In order to circumvent export controls in each country, various majors are taken. Attempting to conceal the end user by using multiple companies and brokers is observed in some cases.
- Note that there is a possibility that there may be companies and individuals even in Japan who cooperate with foreign countries in unlawful procurement.
- It is important to confirm that the business of the ordering party matches the products sold, and that there is nothing suspicious about the order quantity, intended use, end users, etc.

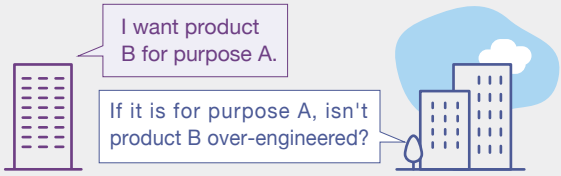
Other possible examples

Multiple inquiries for the same product at the same time



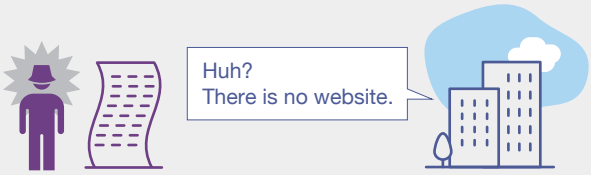
Possibility of the end users being the same?

Mismatch between intended use and product specs



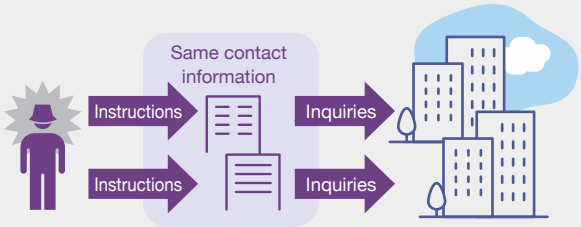
Concealing the real intended use?

There is no website for the ordering company.



Possibly the ordering company does not exist?

Same contact information for different companies

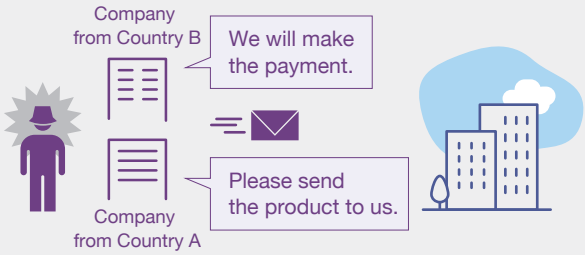


Avoiding regulatory action?

Sudden change of end user

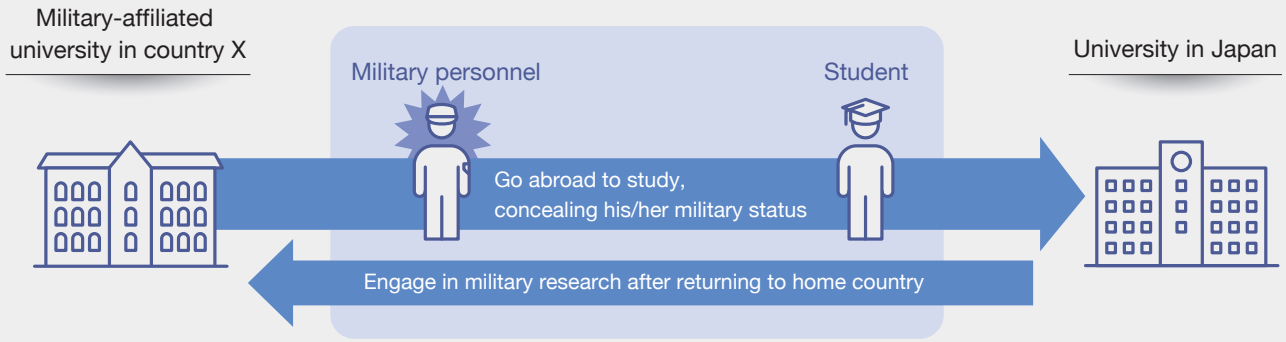
Concealing the end user?

Discrepancy between ordering company and payer



Concealing the intended use?

3 Sending students and researchers



Cases that actually occurred

Case 1:

A former student who was enrolled at a military-affiliated university in China was indicted in 2020 for fraudulently obtaining a US visa by concealing the fact that she was an active-duty soldier, among other charges. It appears that she was gathering information on US military projects etc. while engaged in research in physics and other fields at a US university.

Case 2:

A researcher from a Chinese military-affiliated university, who was engaged in several military research projects in China, received a research grant from the Norwegian government under the guise of new energy research and engaged in hypersonic-related research while at a Norwegian university. The researcher listed the title of the fictitious research institute in the paper.

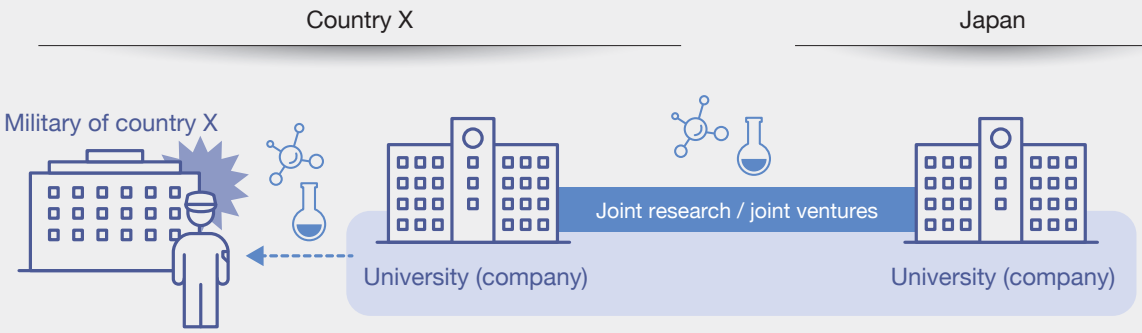
Case 3:

There are several researchers who are engaged in military research in foreign countries after being enrolled in universities and research institutes in Japan.

Point

- There is a possibility that overseas researchers and students may attempt to enter a country by concealing their research intentions and some of their backgrounds.
- When handling important technologies in a laboratory management of research data etc. is also important.
- There is a risk that technologies provided to foreign students and researchers may be used to develop and improve the performance of weapons such as missiles and fighter aircraft in their countries.

4 Joint research and joint ventures



Cases that actually occurred

Case 1:

In 2019, the US authorities placed on the Entity List the joint ventures between companies affiliated with companies developing supercomputers in China and a US company.

Case 2:

The U.S.-China Economic and Security Review Commission (USCC) noted in 2019 that "China has been aggressively acquiring technology through joint research and other means, especially from the United States and its allies and partners."

(Note: The U.S.-China Economic and Security Review Commission (USCC) was established by the US Congress to monitor and study the impact of US-China economic relations on national security and report to Congress.

Case 3:

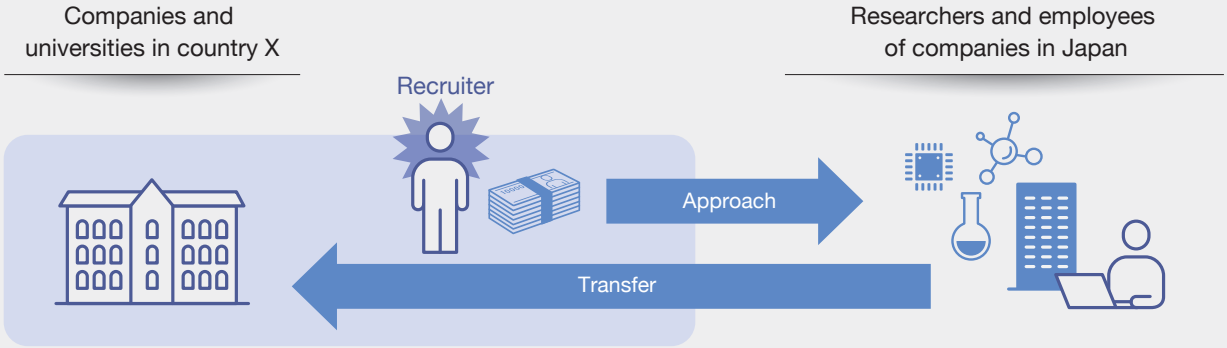
In 2021, the US think tank "C4ADS" suggested in a report that there are unexpected risks in interacting with Chinese university researchers, noting that "some Chinese university researchers belong to joint ventures between universities and defense conglomerates."

(Note: C4ADS is a Washington, D.C.-based non-profit organization that conducts analysis on security and other issues.

Point

- If the partner of the joint research or joint ventures has contacts with the munitions industry of the country of concern, there is a risk that the results of the research or project may be diverted to military use by the country.
- There is a risk that, through joint research and joint ventures, engineers involved in such research and projects may become targets of recruitment.
- With regard to joint research and joint ventures with foreign parties, it is important to confirm the source of research funds and conduct risk assessment.

5 Recruitment of human resources



Cases that actually occurred

Case 1:

In 2013, Japanese researcher A participated in a Chinese talent attraction program and moved to a research center at a university that is closely associated with the Chinese People's Liberation Army. Many prominent researchers from outside of China, including those from Japan, are among the executives of the research center.

Case 2:

In 2015, the South Korean authorities indicted A, an executive at an automobile-related company, for leaking technologies for the production of an inspection device for automobile transmissions to a Chinese company. A took the company's materials and transferred to the Chinese company after being offered conditions such as "double annual income" and "provision of an apartment" from the Chinese company. Thereafter, he continued to request and receive the latest drawings from his former colleagues.

Case 3:

In 2020, the US authorities arrested researcher A, an authority in the field of chemical biology, for receiving tens of thousands of dollars a month in salary and living expenses from a university under the influence of the Chinese People's Liberation Army but concealing it to receive research funding from the United States to continue his research.

Point

- Highly skilled professionals are targeted for recruitment in a wide range of fields.
- In addition to researchers, other individuals with access to critical technologies may be selected as targets for recruitment.
- In solicitation, attractive conditions such as high compensation, housing, and positions may be offered.
- Contracts may be signed that unilaterally benefit the country of concern.

6 Espionage activities

Cases that actually occurred

Case 1:

The US authorities indicted Chinese intelligence officer A in 2018 for conspiring to steal information from US aerospace companies. A apparently encouraged his target to visit China under the guise of asking him to give a lecture at universities and paid him for his travel and rewards.

Case 2:

The US authorities arrested Chinese-American citizen B in 2019 for passing information to Chinese intelligence officers. B apparently passed information related to US security obtained from sources to Chinese intelligence officers between 2015 and 2018.

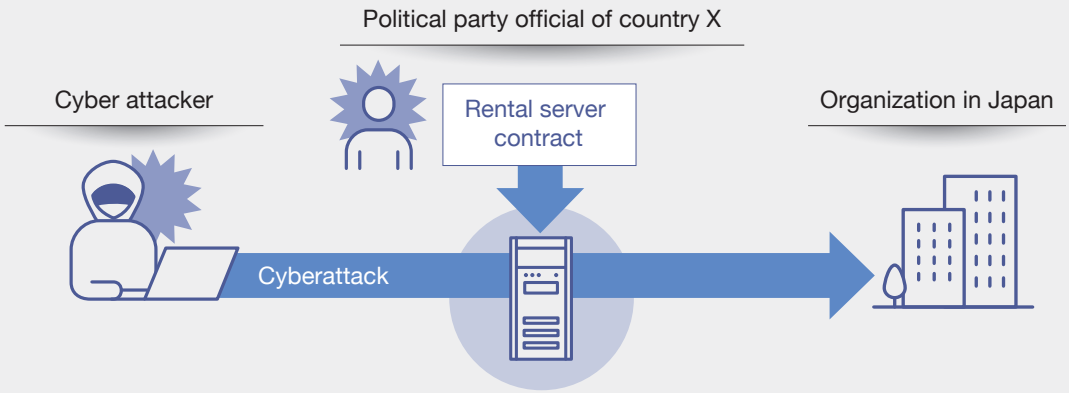
Case 3

In 2020, a former employee of a Japanese telecommunications company, C, was arrested on suspicion of violating the Unfair Competition Prevention Act for accessing the company's server and unlawfully obtaining data. It appears that C began to respond to requests from a former deputy representative of the Trade Representative of the Russian Federation in Japan during a series of meetings with the former deputy, which eventually led to the unlawful acquisition of the data.

Point

- Intelligence officers and others use venues such as industry exhibitions and lectures to identify important information, technologies, and human resources, and then select individuals to be targeted.
- Intelligence officers and others focus on building relationships with targeted individuals by contacting them under the guise of coincidence, whether in public or private life, and subsequently setting up various pretexts for "one-on-one" meetings with them.
- Intelligence officers and others gradually escalate their demands and eventually apply pressure in an attempt to obtain important information.

7 Cyberattacks



Cases that actually occurred

Case 1:

In 2015, an employee of an organization in Japan opened a file with malware attached to an email, resulting in the remote control of a PC terminal from the outside and the leak of approximately 1.25 million personal information of subscribers.

Case 2:

Regarding a cyberattack (in 2019) against a major Japanese electronics manufacturer, it was found that out of approximately 20,000 data files containing defense-related information that may have been leaked to outside parties as a result of the attack, there were approximately 60 data files that may have had an impact on national security.

Case 3:

In 2021, a Chinese Communist Party member who was staying in Japan at the time was referred to the public prosecutor on suspicion of unauthorized creation and use of private electronic or magnetic records for having contracted under a false name for a rental server used in cyberattacks against Japanese organizations and others. It was pointed out that "Tick," a China' s cyber threat entity with the support of the Unit 61419 of the Chinese People's Liberation Army, was likely involved in this incident.

Point

- Cyberattacks exploit "vulnerabilities" (flaws and weaknesses) in computer systems, including unknown "zero-day vulnerabilities," as well as unlawful access to systems by exploiting gaps in human minds, deceiving, and misleading them.
- It is important to understand the status of PCs, smartphones, and other devices in use, as well as software and application versions, and update them to the latest versions.
- Clicking on attachments or URLs in suspicious emails, SMS, social media, etc. should be strictly prohibited.

Column

"Economic Coercion" by Countries of Concern

Countries of concern are said to be engaging in "the use, or threat to use, measures of an economic character taken to induce a target state to change some policy or practices" (source: "Oxford Public International Law"[*1]), and these activities are called "Economic Coercion."
"The German Marshall Fund (GMF)[*2]," a US think tank, has compiled a database of major cases of "economic coercion" by China and Russia, numbering 130 cases (70 by China and 60 by Russia) (as of March 28, 2022).

Norway

In 2010, the Nobel Peace Prize was awarded to a jailed Chinese human rights activist Liu Xiaobo for his "long and non-violent struggle for fundamental human rights in China."

China

Tightened quarantine on Norwegian salmon, effectively restricting imports. Norwegian salmon market share in China dropped from 92% to 29%.

The Nobel Prize: Diploma and medal presented to Liu Xiaobo that were placed on an empty chair" (December 10, 2010) (Photo courtesy of AFP=Jiji Press)

Moldova

Strengthened political, economic, and security ties with the EU after signing (2014) an "Association Agreement, including the Deep and Comprehensive Free Trade Area (DCFTA)" with the EU.

Russia

Increased the price of natural gas exported to Moldova from $550 to $790 per m³ and partially suspended supply.

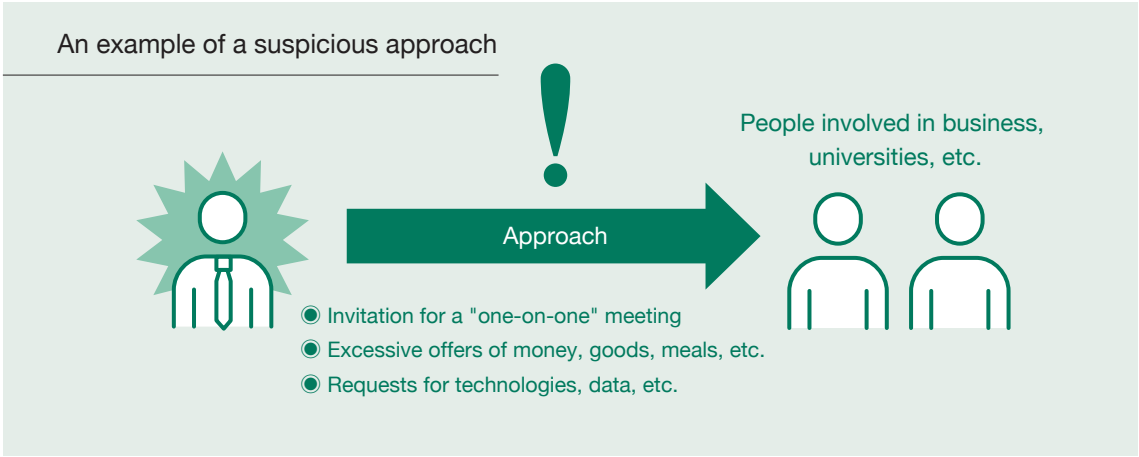
Natural gas pipelines from Russia (image courtesy of Kyodo News)

Japanese companies may be subjected to "economic coercion."

※1 Barry E Cartert. "Economic Coercion". Oxford Public International Law. http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1518?prd=EPIL#:~:text=As%20a%20starting%20point%2C%20the,structure'%20(Lowenfeld%20698). (2022-04-05)
※2 "Tool: Economic Coercion". Alliance for securing democracy, The German Marshall Fund of the United States. http://securingdemocracy.gmfus.org/asd_tools/strategic-economic-coercion/. (2022-04-05)

Response to Suspicious Approaches

In the course of normal economic or research activities, there is a risk that you may be approached by other parties, whether public or private, who may request persistently, for example, one-on-one meetings, or ask you to provide technologies, data, and products in return for excessive favors such as money, goods and meals.
In such cases, if you identify anything even slightly suspicious, it is important to keep in mind that it should never be handled by an "individual" but by an "organization."



Key points in responding when approached in a suspicious manner

- ✓ Report and consult with your supervisor, colleagues, or the department in charge.
- ✓ Do not give out personal contact information such as private cell phone numbers or email addresses.
- ✓ Avoid detailed references to your own or your colleagues' work responsibilities.
- ✓ Be aware that there may be contacts that take advantage of personal kindness (e.g., giving directions to a foreigner who is lost), etc.
- ✓ Avoid making individual appointments for meetings. Always have meetings with more than one person after consulting with the supervisor or the department in charge of the case.
- ✓ To the extent possible, efforts should be made to obtain specific information about the nature of the business and objectives of your counterpart.

Appropriate Information Management

There is a risk that technologies, data, and products may be unintentionally leaked outside the organization due to inadequate information management within the organization, and efforts toward appropriate information management are required.

An example of measures taken by an organization

Physical Protection

Restrict access to sensitive information

Physically restrict the taking out

Psychological Protection

Ensure visibility in the workplace, etc.

Display "Secret"

Promote education within the organization

An example of measures taken as an individual

Always update the OS on the terminal to the latest version.

Avoid posting business or personal information (e.g., addresses, phone numbers, email addresses) on social media sites and other sites as much as possible.

Do not click carelessly on URLs or attached files of emails, SMS, social media, etc. that you receive, including those that appear to be from acquaintances.

Main points to consider when managing information within the organization

- Establish rules for the handling of information and clarify the matters to be complied with.
- Properly manage equipment and files that handle information to prevent loss or taking out.
- Restrict those who have access to information and prevent viewing or theft by outsiders.
- Develop a system to promptly report within the department a suspicious access received from outside, and publicly announce the incident to prevent similar incidents from occurring elsewhere.
- Regularly conduct internal organizational education, including training on information management, to raise the awareness of those who handle information.

Public-Private Partnership and Information Dissemination

Importance of Public-Private Partnership

In order to prevent leak of technologies, data, and products, it is necessary for companies, universities, etc., and public agencies to understand trends of concern and respond appropriately.
Recognizing that strengthening public-private cooperation is indispensable for preventing the leak of technologies, data, and products, the Public Security Intelligence Agency has established a contact point for communication and consultation regarding economic security and contributes to preventing the leak of technologies, etc. from companies, universities and other institutions by sharing various findings on suspicious approaches, etc. through various information dissemination.

Information Dissemination

Economic Security

The Public Security Intelligence Agency has opened a special feature page on economic security on its website, and publishes educational videos, pamphlets, and other materials. If you are a person in charge at a company or university, etc. who wish to have a lecture on the contents of this pamphlet or economic security, please contact the Public Relations Coordination Office of the Agency (See below for contact information).

Publication of Educational Videos

A video summarizing the risks of technology leak has been released.

Trends Related to Economic Security

The special feature page provides information on relevant overseas trends by year and month.

Ensuring Economic Security

This pamphlet is also available on the Agency website.

Giving Lectures

Upon request, we give lectures on topics such as preventing the leak of technologies, data, and products.

Contact Point for Communication and Consultation for Economic Security

https://www.moj.go.jp/psia/kouan_mail_keizaianpo.html

E-mail **psia-es@i.moj.go.jp**

Website of the Public Security Intelligence Agency

The web pages of the Public Security Intelligence Agency post related laws and regulations under the Agency' s jurisdiction, its history, and tasks, and show situations at home and abroad in each of the following categories: "Economic Security Special Feature Page," "Aum Shinrikyo," and "Situations occurring tied to terrorism and relevant affairs in the world." It also notifies recruitment information and event information on job fairs for new recruits, which are conducted nationwide. We hope you will visit our website.

https://www.moj.go.jp/psia/ Public Security Intelligence Agency Search

Official SNS Accounts of the Public Security Intelligence Agency

The Official Twitter account of the Public Security Intelligence Agency and the Agency's official YouTube channel contain information about the Agency's measures and initiatives, and are used to distribute information that the Agency wants to announce. We hope you will view this information, together with the information available on the Agency's website.

Official Twitter account **@MOJ_PSIA**

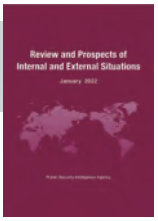
Offcial Twitter account (for recruitment) **@PSIA_recruit**

Official YouTube channel **PSIAchannel**

Publications

Review and Prospects of Internal and External Situations

This is a review of situations concerning public safety both in Japan and abroad over the past year, as well as an outlook on the future.



Review and Prospects of Internal and External Situations (January 2022)

Handbook of International Terrorism

This is a summary of current trends in international terrorism, profiles of international terrorist organizations and their moves, and the state of terrorism by region.

Handbook of International Terrorism 2021

Overview of Threats in Cyberspace

This is a summary of threats posed by cyberattacks in recent years, their patterns, actors, modus operandi, and countermeasures.

Overview of Threats in Cyberspace 2022

Organization and Network

The organization of the Public Security Intelligence Agency consists of its internal departments, an affiliated organ, and regional bureaus. The internal departments comprise the following three departments: the General Affairs Department, the First Intelligence Department, and the Second Intelligence Department. The agency has the Public Security Intelligence Agency Training Institute as its affiliated organ, and the Public Security Intelligence Bureaus and Public Security Intelligence Offices comprising the regional branches across Japan.

1. Public Security Intelligence Agency (Headquarters)
2. Public Security Intelligence Agency Training Institute
3. Hokkaido Public Security Intelligence Bureau
4. Tohoku Public Security Intelligence Bureau
5. Kanto Public Security Intelligence Bureau
6. Chubu Public Security Intelligence Bureau
7. Kinki Public Security Intelligence Bureau
8. Chugoku Public Security Intelligence Bureau
9. Shikoku Public Security Intelligence Bureau
10. Kyushu Public Security Intelligence Bureau

●…Public Security Intelligence Offices

Public Security Intelligence Agency
Central Government Building No.6 1-1-1 Kasumigaseki, Chiyoda-ku, Tokyo 100-0013 TEL: 03-3592-5711 (main)

Protecting the People with the Power of Intelligence

PSIA 公安調査庁
PUBLIC SECURITY INTELLIGENCE AGENCY

2022.05