PROTECTION OF STRATEGIC AND DUAL-USE TECHNOLOGIES

A TAKE ON THE CURRENT SITUATION AND VARIOUS APPROACHES

JAN FAMFOLLET

2022

REPORT

EUROPEAN VALUES CENTER FOR SECURITY POLICY

European Values Center for Security Policy is a non-governmental, non-partisan institute defending freedom and sovereignty. We protect liberal democracy, the rule of law, and the transatlantic alliance of the Czech Republic. We help defend Europe especially from the malign influences of Russia, China, and Islamic extremists.

We envision a free, safe, and prosperous Czechia within a vibrant Central Europe that is an integral part of the transatlantic community and is based on a firm alliance with the USA.

Author:

Jan Famfollet

Keywords:

- **Dual-use technologies** are goods, software, or technology (documents, diagrams, etc.) that can be used for both civil and military applications. They can range from raw materials to components and complete systems, for example, aluminum alloys, bearings, or lasers. They could also be items used in the production or development of military goods or chemical, biological, or nuclear weapons, for example, machine tools, chemical/manufacturing equipment, or computers (GOV.UK, 2017).

CONTENTS

EXECUTIVE SUMMARY

- In the context of technology transfer, possible misuse of dual-use technologies, and intensified geopolitical competition, democratic countries need to ensure that sensitive, dual-use, and otherwise strategic technologies, regardless of their public or private origin, do not fall into the wrong hands.
- The main concern in this regard is China and its rising multifaceted geostrategic aspirations, which have technology supremacy at their core. China uses myriad illegitimate and illegal means to acquire foreign technology and know-how with the aim of enriching its military research, ultimately turning it against the countries from which these technologies were originally acquired.
- Therefore, democratic countries need to carefully assess which of their emerging technologies—not necessarily yet regulated as military, dual-use, or critical infrastructure—have strategic potential and then implement measures to protect them and—if they wish to use them fully to their geopolitical advantage—support their development.
- The examples of specific countries and regions (the US, EU, Japan, Taiwan, China) show that each has defined a specific scope of strategic technologies and deployed specific measures for their protection and support.
- These scopes are derived from the national innovation environments and different comparative advantages, needs, and interests of each territory.
- One way to identify strategic technologies is to look at what foreign predators consider strategic in a particular economy and what they seek to retrieve.
- For example, in recent years, Chinese "science and technology diplomats" have focused primarily on biotechnology and pharmaceuticals, on artificial intelligence and machine learning, and on technologies with military applications possessed by the US and its allies.
- The state thus needs to have in place good analytical and (counter)intelligence capacities to expose foreign actors' industrial and research espionage objectives and technology targets. Such knowledge then enables the proper adaptation of national technology policies.
- Potential restrictive measures include the following: export controls, import restrictions, inbound investment screening, outbound investment screening, inclusion of problematic entities on an "entity list," application of financial sanctions, and so forth.
- Potential supportive measures include the following: subsidies and tax incentives, special public-private investment funds, public guarantees, and so forth.

- A special regime for designated sectors can further include the following: strengthening supply chain security and integrity, ensuring the security of key basic infrastructure, helping enhance cyber security, expanding public-private technological cooperation, dialogue and information/data sharing, protecting research and keeping certain patents confidential, incentivizing diversification, and reshoring.
- There is a limit to what is compatible with state aid regulations as supportive measures essentially constitute industrial policies. However, national security is a natural basis for state aid exemptions.
- There is also a limit to what one country can do alone. Therefore, international coalition-building among like-minded countries is essential to ensure collective resilience.
- Finally, there is a limit to what can be achieved by relying on protective measures. Therefore, an active supportive approach and international collaborative efforts are needed to accelerate democratic countries' technological development and international competitiveness and to leave foreign adversaries behind.

INTRODUCTION

Modern technologies have a growing impact on the lives, prosperity, and security of citizens. Moreover, the security of every state is becoming increasingly dependent on such technologies. The development of new technologies creates enormous potential as they play a crucial role in both international economic and military competition. As such, they bring new risks to national security and can significantly impact the future global balance of power. This trend is apparent from the rising multifaceted geostrategic aspirations of the People's Republic of China (PRC) in global affairs and its extensive engagement in malicious activities, mainly technology and intellectual property (IP) transfer and theft, which have developed into a full-fledged technological adoption race (Bagge & Havránek, 2021).

The governments of individual countries have embraced this reality in different ways and formulated their technology policies according to their security and foreign policy interests, taking into account the domestic context and capabilities. The purpose of this report is to reflect on the various national strategies and inform policy debates in countries that do not yet have any relevant technology policy in place or are considering updating their current one.

THE ISSUE OF TECHNOLOGY TRANSFER

Sensitive, dual-use, or otherwise strategic technologies, regardless of their public or private origin, are of paramount importance and may have significant impacts. Therefore, it is in the vital interest of every country to ensure that they, at the very least, do not fall into the wrong hands. Such misappropriation can easily happen through myriad ways, including cyber-attacks and economic espionage (resulting in IP theft) or simply through inbound investments, mergers and acquisitions, export, or outbound joint ventures. Undue technology transfer is also increasingly enabled by academic exchanges between universities and research institutions.

Naturally, the transfer of technology is not necessarily always bad. Continuous technology exchanges may be beneficial and desirable if they are carried out in commercial or academic environments that are transparent and fair, between countries and parties that respect the same rules and share the same values. In such cases, it may help the concerned countries develop cost-effective technology bases, for example, in the defense industry and other sensitive industries.

However, this does not hold for technology transfer that is carried out on the basis of hidden state agendas, through covert ways, and using illegitimate—or outright illegal—means to ultimately serve political objectives that are hostile to the particular country from which the technology was acquired and that even include preparing for future conflict with that country.

In any case, the transfer of sensitive technology, be it due or undue, has strategic implications. Competition around the emerging technologies is becoming a new frontier of global geopolitical competition (Gui, 2022). Therefore, state administrations have gotten involved in the technology sphere and increasingly submit select technologies and sectors to conscious state (technology) policies in order to ensure their protection, and—if governments wish to use these technologies' potential to their advantage—support.

THE POSITIONING OF TECHNOLOGY WITHIN ECONOMIC SECURITY

Technology is a frequent focus of economic statecraft, which can be defined as the use of economic means to pursue foreign policy goals (Baldwin, 2016). Using economic statecraft in an offensive manner amounts to economic warfare whereas a defensive expression of economic statecraft is economic security. Some authors claim that economic statecraft itself is already a rather offensive concept that coincides with economic coercion, that is, using one's own economic advantages or superiority as leverage to impose one's political will and values on others (Suzuki, 2022a), and so is distinct from the defensive economic security concept.

The essence of economic statecraft in any of its forms lies in the nexus between economics and security. The most pronounced example of fields where economics and security intersect is technology—in particular, technology that serves both civilian and military purposes, "dual-use" technologies (e.g., semiconductors, navigation systems, drones, etc.) that are critical for both security and possible offensive military buildup and whose importance is growing.

Security through non-proliferation of technology is one of the possible meanings of economic security (alongside the security of supply chains and others). It aims to avoid a situation where the lives and property of citizens are jeopardized by an adversary country's military capabilities enhanced by the proliferation of technologies through trade and other means (Suzuki, 2022a). Practical measures to prevent the outflow of cutting-edge and sensitive technologies applicable in military research include non-disclosure of sensitive patents or bolstering relevant institutions' cyber security.

Some current practical approaches to economic security also emphasize its "active" dimension, that is, ensuring economic security by deliberately and consciously strengthening the industrial and technological base of the country to enhance its international standing and its indispensable role in global supply chains. The rationale is to make the country less vulnerable, for example, to economic coercion. By giving the original object of mere protection also an active role in the process, economic security may then be understood as protecting the national economy but also as technology and the economy serving security interests.

When assessing the importance of technologies in a more comprehensive concept of national security, it leads the state to formulate a technology strategy. Individual technology policies then focus on the protection and/or support of designated technologies.

IDENTIFYING STRATEGIC SECTORS

The theft or acquisition by other means of sensitive research or IP by a geopolitical adversary can threaten national security. Therefore, states need to carefully assess which of their technologies have strategic potential and then take steps to protect them and—if countries wish to use these technologies fully to their geopolitical advantage—to support their development. The very first step is to identify new technologies of strategic importance, which is, however, also one of the biggest challenges.

Certain sectors of national economies are traditionally regulated. First layer of sensitive technology designation is rather apparent: **military items** such as weapons and ammunition are typically heavily regulated industries in every country. Another category usually defined and subject to national regulations is **critical infrastructure** and its elements, typically associated with the energy, water management, health care, transport, communication, and information systems; public administration; the financial system; and sometimes the media.

Other technologies may be less apparently sensitive but still make it on various export control lists. These are **dual-use items**, that is, goods, software, and technology (documents, plans, etc.) that can be used for both civil and military applications. They can range from raw materials to components and complete systems, for example, aluminum alloys, bearings, or lasers. They could also be items used in the production or development of military goods or chemical, biological, or nuclear weapons, for example, machine tools, chemical/manufacturing equipment, and computers (GOV.UK, 2017).[1] However, properly assessing all new technologies and designating concrete ones as dual-use pose challenges due to the current limited knowledge of their future potential and applications.

Those that are not yet classified as dual-use but which apparently possess great potential for the future may be called strategic technologies. These may consist of emerging, disruptive, advanced, and otherwise sensitive technologies outside the bounds of military equipment, currently designated dual-use technology, and critical infrastructure. Even though many strategic and effectively dual-use technologies are developed by private companies, **sectors of strategic interest**, such as semiconductors, new energy, and advanced materials, tend to have high levels of state influence (Irwin-Hunt, 2022).

1 Under a voluntary pact between forty-two nations called the Wassenaar Arrangement, the US and its allies aim to curb the spread of dual-use technology. For example, they have harmonized controls over the flow of chip technology to China (Lee, Shirouzu, & Lague, 2021).

In countries where no special regime for advanced technologies exists yet, the big challenge is to properly identify sectors that would fall under the scope of the new instruments of economic and research security policy. This scope differs from one state to another as the national innovative environments of national economies differ as well.

Some examples of sectors or technologies that may be considered strategic include quantum computing, advanced materials, synthetic biology, artificial intelligence (AI) and machine learning, robotics, optoelectronics, smart grids, big data, cloud computing, sensitive data processing and storage, energy storage, cyber security, semiconductors, aviation, space, nanotechnology, biotechnology, pharmaceuticals, and medical research.

The specific selection depends on the individual state's preferences, national security considerations, and comparative advantages.

One specific approach to identifying strategic technology is to look at what foreign predators consider strategic in the particular national economy and what they seek to retrieve. For instance, Chinese "science and technology (S&T) diplomats" stationed at PRC embassies and consulates act as part of the PRC's broader strategy to acquire foreign technology. They file hundreds of official reports annually, the study of which can indicate which types of technologies the Chinese government is most focused on acquiring and from where.[2] The Center for Security and Emerging Technology (CSET) has examined these materials and produced the study "China's Foreign Technology Wish List." They found that the fields of particular interest to the PRC from 2015 to 2020 were **biotechnology** and **AI**. PRC diplomats also frequently sought to acquire components and systems used by the **militaries** of the US and US allies. The most targeted countries were Russia, the US, the United Kingdom, Japan, and Israel. As regards success rate, roughly around 50 percent of the enterprises identified by S&T diplomats ultimately formed partnerships with Chinese counterparts or otherwise exposed their IP (Fedasiuk, Weinstein, & Puglisi, 2021).

This latter approach points to the need for the state to have in place good analytical and **(counter)intelligence** capacities to effectively expose foreign actors' industrial and research espionage objectives and technology targets. Such knowledge would then enable the proper **adaptation** of national technology policies.

2 "S&T diplomats form the outward-facing portion of China's broader technology transfer ecosystem, and monitor scientific breakthroughs, technology enterprises, and other forms of innovation that may be of interest to the Chinese government" (Fedasiuk, Weinstein, & Puglisi, 2021).

INSTRUMENTS OF TECHNOLOGY PROTECTION AND SUPPORT

After identifying its comparative advantages and the sectors considered critical, core, or strategic, a state can implement many strategies to protect and support them.

On top of traditional tools such as military export control and non-proliferation regulations, many countries have recently implemented or strengthened their foreign direct investment (FDI) screening mechanisms that aim to shield potentially transformative technologies from foreign acquirers. An important factor is then the capacity of national authorities to monitor and screen potentially large numbers of merger and acquisition (M&A) deals.

Besides export controls and FDI review, states can do the following: impose import restrictions, impose restrictions on outbound investments in problematic countries, include problematic entities on the country's "entity list" (leading to market restrictions and the effective prohibition of selling and re-selling domestically sourced goods and technologies[3]), or apply financial sanctions.

Apart from applying these traditional restrictive tools, states can also develop supportive measures for the designated sectors. This support can take the form of subsidies and tax incentives (to motivate desired behavior on the part of private industries) or special public-private investment funds with substantial government contributions and/or guarantees. Free-market economies are limited in providing such support because they need to ensure such programs, which are essentially **industrial policies**, comply with national or supranational regulations on state aid. However, in practice, regulation may be circumvented through security exemptions.

The state can thus create a more-or-less comprehensive **special regime** for designated technologies and industries consisting of both protective and supportive measures. Such a regime would be tailor-made to every country. It can, on top of the application of traditional economic security tools (see above), consist of the following: strengthening enterprises' supply chain security and integrity, ensuring the security of their key basic infrastructure, helping enhance cyber security, expanding public-private technological cooperation, dialogue and information/data sharing, protecting research and keeping certain patents confidential, conducting outbound investment screening, incentivizing diversification and reshoring, and so forth.

Public-private cooperation is essential. The government and the private sector should work together to achieve economic security, with the government making companies get involved in policy implementation by engaging in extensive communication, promoting their business activities, and controlling them at the same time (Suzuki, 2021). If the government ensures

3 In the case of the US economy, these restrictions may result in the significant impairing of the listed company's supply chain and business operations.

striking a balanced policy between industrial competitiveness and national security (Suzuki, 2022b), such an enhanced regime for strategic industries can contribute to protection, long-term sustainability, and the development of the designated technologies.

NATIONAL STRATEGIES OF SELECT COUNTRIES

The following section provides a brief overview of the national strategies of some of the most important global actors.

United States

One of the key documents covering strategic technologies is FIRRMA (The Foreign Investment Risk Review Modernization Act), which introduced an expanded export control process for **"emerging and foundational"** technologies and increased scrutiny of Chinese investment in the US. Furthermore, the NCCDA (The National Critical Capabilities Defense Act) defines **national critical capabilities** as production, services, and supply chains in four sectors: medical supplies and PPE (Personal Protective Equipment), disaster recovery, military and intelligence, and critical infrastructure – an umbrella term that itself encompasses sixteen subsectors ranging from agriculture to nuclear power (US-China Investment Project, 2022). **Critical industries** identified under the National Network for Manufacturing Innovation include but are not limited to energy; medical; communications, including electronic and communication components; defense; transportation; aerospace; robotics; artificial intelligence; semiconductors; shipbuilding; and water, including water purification (Casey & Cornyn , n.d.).

Another important document is the **Innovation and Competition Act**, which aims at protecting US innovation and strengthening national competitiveness. It interconnects academic research, government grants, venture capital, and free market competition. Additionally, it funds the National Science Foundation (NSF), through which it awards grants to strategic technologies (Harrington & McCabe, 2021).

The US also restricts semiconductor transactions with the PRC with a view to delaying the strengthening of the Chinese military and economy by making unavailable to the country semiconductors manufactured with advanced microfabrication technology while protecting technologies in which the US and Western countries excel (Suzuki, 2022a).

At the same time, a new bill called the **CHIPS for America Act** will provide $52 billion in subsidies to the semiconductor industry in the US to protect the country from supply shortages and make the US more competitive with China (Garver, 2022). The vast majority of financial assistance is to build domestic semiconductor facilities, followed by funding chip research and workforce development (Flatley & Wasson, 2022).

European Union

Within the EU, there have traditionally been export controls on weapons and military equipment. Further export controls cover goods and intangibles like software, networks, and other types of virtual environments. Export control regime is determined by multilateral platforms and related agreements. There is also an EU regulation (2021/821) on dual-use technologies covering nine umbrella categories: special materials and related equipment; materials processing; electronics; computers; telecommunications and "information security"; sensors and lasers; navigation and avionics; marine; aerospace and propulsion. The EU coordinates its approach in this area with the US via the Trade and Technology Council (TTC).

EU member states also receive information from each other on what is happening in other member states through the new FDI screening coordination mechanism, thanks to which they can share information on potential risks. Eighteen member states have already implemented new FDI screening mechanisms or amended existing ones, while the other member states (with two exceptions) are about to follow this trend. There are also efforts to develop a European approach to cyber surveillance.

The EU now accounts for 10 percent of the global market for microchips, which are strategic assets for key industrial value chains. The EU wants to double its global share of the semiconductor market to 20 percent (European Commission, 2022). **The European Chips Act**, announced in February 2022 and aiming to address the semiconductor shortage and strengthen the EU's technology leadership, should help do just that. Together with its member states, the EU wants to mobilize public and private investments of over €43 billion, mainly to subsidize (high-end) semiconductor manufacturing and strengthen the EU's research and development (R&D) framework. Key elements of the strategy include giving the European Commission power to manage supply chains in emergencies and building international partnerships in semiconductors.

The EU is also undertaking a similar initiative in the field of AI.

Japan

In 2020, economic security proposals made by the Liberal Democratic Party (LDP) identified Japan's **strategic infrastructure industries** and provided an analysis of their vulnerabilities. These sectors are energy, telecommunications, transport, food, medicine, finance, and construction (Takahashi, n. d.).

In the area of business, sixteen core designated sectors are protected by an FDI screening mechanism, which has been recently strengthened. These sectors include weapons, aircrafts, space, nuclear facilities, dual-use technologies, cyber security, electricity, gas, telecommunications, water supply, railway services, and oil (Smith & Ning, 2020).

There is also a complex system of reshoring aimed at returning the production of **high value-added goods** from the PRC to Japan and diversifying the rest of the production base to other countries. Overall, Japan is spearheading efforts to establish a functional institutional architecture and to enact fundamental rules that should ensure and enhance its economic security. The new Economic Security Promotion Act enacted in 2022 focuses on 1) strengthening supply chain security, 2) protecting critical infrastructure, 3) fostering public-private technological cooperation, and 4) making sensitive patents classified.

Taiwan

Taiwan has also deliberately identified its strategic technologies. Taiwan has a category of **strategic high-tech goods (SHTGs)** that are subject to special regulations. Under the Taiwanese Foreign Trade Act, export restrictions apply to these SHTGs (in addition to military equipment and dual-use items); they cannot be exported without permission, and the recipients must be screened against the country's Entity List (TW Ministry of Economic Affairs, 2017; TW Ministry of Economic Affairs - BFT, n.d.).

China

China conducts systematic worldwide open-source monitoring of technologies that could be useful for its national strategies. S&T diplomats are deployed all over the world to establish relationships with professors from Western universities to get access to their knowledge and research.

At the same time, China protects its **key sectors** through FDI screening. Apart from the military or national defense-related businesses, the covered sectors include key agricultural products; key energy and resources; key major equipment manufacturing; key infrastructure; key transportation services; key cultural products and services; key information technology and internet products and services; key financial services; key technology; and other key sectors.

What is considered **"key"** is not set out in any regulation, leaving the "Working Office" with the discretion to decide in line with changes in the PRC's foreign investment policies or national security outlook from time to time (Wu & Wut, 2021).

COLLECTIVE RESILIENCE

There are limits to what one country can do alone. International technology cooperation is essential to ensure synergies between scattered knowledge and establish global technology standards. Therefore, like-minded countries should build coalitions to increase collective resilience with a view to "put [foreign adversaries] down and speed [themselves] up" (Suzuki, 2022a).

A prominent example of such international technology cooperation is the **Quadrilateral Security Dialogue (QUAD)**, which aims to ensure that technology is developed and used in line with the principles of a free, open, and resilient Indo-Pacific, based on shared democratic values and respect for universal human rights. QUAD countries (Australia, India, Japan, and the US) consider writing new rules for critical and emerging technologies to be a key imperative. QUAD efforts focus on four issues: technical standards, 5G diversification and deployment, horizon scanning, and technology supply chains. QUAD countries will also work together on emerging technologies, space, cybersecurity, advanced communications, AI, and advanced biotechnologies (Rajagopalan, 2022).

CONCLUSION

In the current international environment, where new technologies are increasingly important to people's lives and national security, and given the growing technology competition between China and the free world, democratic countries are discovering it is essential to identify, protect, and develop critical technologies, and to enhance the resilience of essential industries.

To date, it is difficult to evaluate whether a specific country has a best designed regime for the protection and support of strategic technologies in place, as each country has a specific innovation environment and different comparative advantages, needs, and interests. This also determines the specific scope of technologies and sectors of the national economy that a given government chooses to consider as strategic.

For countries that have not yet embarked on the process of identifying their strategic technologies and subjecting them to enhanced protection and support, a helpful benchmark for identification is to study what the economic and scientific espionage activities of foreign adversaries, essentially of the PRC, focus on in the target economy. Yet countries need to carefully strike a good balance between effective protection and support of their technologies on the one hand, and unjustified and ultimately harmful protectionism on the other.

International technology cooperation is essential to ensure synergies between scattered knowledge and to establish global technology standards. Therefore, like-minded countries should build technology coalitions to increase collective resilience and foster collective technology advancement with a view to "put China down and speed us up."

REFERENCE

Bagge, D., & Havránek, J. (2021, July 18). Technology Adoption: Are we too late to the party? *Small Wars Journal*. Retrieved from https://smallwarsjournal.com/jrnl/art/technology-adoption-are-we-too-late-party

Baldwin, D. (2016). *economic statecraft*. Retrieved from Britannica: https://www.britannica.com/topic/economic-statecraft

Casey, B., & Cornyn, J. (n.d.). *National Critical Capabilities Defense Ac*. Retrieved from https://www.casey.senate.gov/imo/media/doc/one_pager_nccda.pdf

European Commission. (2022). European Chips Act. Retrieved from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

Fedasiuk, R., Weinstein, E., & Puglisi, A. (2021, May). China's Foreign Technology Wish List. *Center for Security and Emerging Technology (CSET)*. Retrieved from https://cset.georgetown.edu/publication/chinas-foreign-technology-wish-list/

Flatley, D., & Wasson, E. (2022, July 27). Chipmakers Get $52 Billion in Senate Bill in Big Win for Biden. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2022-07-27/microchip-funding-bill-passes-senate-in-major-victory-for-biden

Garver, R. (2022, July 21). US Congress Moves Toward $52 Billion in Subsidies for Semiconductor Firms. *Voice of America (VOA)*. Retrieved from https://www.voanews.com/a/us-congress-moves-toward-52-billion-in-subsidies-for-semiconductor-firms/6667675.html

GOV.UK. (2017, February 23). *UK Strategic Export Control Lists*. Retrieved from Department for International Trade - Export Control Joint Unit: https://www.gov.uk/guidance/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items

Gui, Y. (2022, March 19). Moving toward decoupling and collective resilience? Assessing US and Japan's economic statecraft against China. *China International Strategy Review*(4), pp. 55–73. Retrieved from https://link.springer.com/article/10.1007/s42533-022-00097-z

Harrington, J., & McCabe, R. (2021, July 1). What the U.S. Innovation and Competition Act Gets Right (and What It Gets Wrong). *Center for Strategic and International Studies (CSIS)*. Retrieved from https://www.csis.org/analysis/what-us-innovation-and-competition-act-gets-right-and-what-it-gets-wrong

Irwin-Hunt, A. (2022, February 11). EU FDI screening moves beyond China. *FDI Intelligence*. Retrieved from https://www.fdiintelligence.com/content/feature/eu-fdi-screening-moves-beyond-china-80676

Lee, Y., Shirouzu, N., & Lague, D. (2021, December 27). Taiwan chip industry emerges as battlefront in U.S.-China showdown. *Reuters*. Retrieved from https://www.reuters.com/investigates/special-report/taiwan-china-chips/

Rajagopalan, R. P. (2022, July 9). The Growing Tech Focus of the Quad. *The Diplomat*. Retrieved from https://thediplomat.com/2022/07/the-growing-tech-focus-of-the-quad/

Smith, G. M., & Ning, N. (2020, May 22). Japan Moves to Tighten Restrictions on Foreign Investment in Healthcare Industries. *Morrison Foerster (MoFo)*. Retrieved from https://www.mofo.com/resources/insights/200522-japan-restrictions-foreign-investment.html

Suzuki, K. (2021, December 3). What Japan needs to do to boost its economic security. *API Geoeconomic Briefing*. Retrieved from https://apinitiative.org/en/2021/12/03/29186/

Suzuki, K. (2022a, March). Economic Security in the Free Trade Regime. *Society of Security and Diplomatic Policy Studies (SSDP)*. Retrieved from http://ssdpaki.la.coocan.jp/en/proposals/102.html

Suzuki, K. (2022b, March 2). Japan's Economic Security and Semiconductor Industry. *The Japan Institute of International Affairs*. Retrieved from https://www.jiia.or.jp/en/ajiss_commentary/japans-economic-security-and-semiconductor-industry.html

Takahashi, T. (n.d.). Japan's opaque economic security policy agenda. *Australia-Japan Research Center*. Retrieved from https://ajrc.crawford.anu.edu.au/department-news/19756/japans-opaque-economic-security-policy-agenda

TW Ministry of Economic Affairs - BFT. (n.d.). *Export Control (SHTC)*. Retrieved from Bureau of Foreign Trade: https://www.trade.gov.tw/english/Pages/List.aspx?nodeID=298

TW Ministry of Economic Affairs. (2017, October 20). *Regulations Governing Export and Import Of Strategic High-tech Commodities*. Retrieved from Laws & Regulations Database of the Republic of China: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0090013

US-China Investment Project. (2022, January). An Outbound Investment Screening: Regime for the United States? *US-China Investment Project*. Retrieved from https://rhg.com/wp-content/uploads/2022/01/RHG_TWS_2022_US-Outbound-Investment.pdf

Wu, H. H., & Wut, T. (2021, January 4). China enacts new foreign investment security review measures. *Baker McKenzie*. Retrieved from https://www.bakermckenzie.com/en/insight/publications/2021/01/china-enacts-new-foreign-investment-security

WWW.EUROPEANVALUES.CZ