THE 10TH JOINT INDUSTRY OUTREACH SEMINAR

ON STRATEGIC TRADE MANAGEMENT - SINGAPORE 2022

Critical Technology Protection Best Practices

Monday, 12 September 2022

Critical Technology Protection Best Practices

- **What is "critical technology"?**
  - Generally defined as technologies that can significantly enhance or pose risk to national interests,
  - Relationship to "strategic" (or export-controlled) technology
  - Relationship to "emerging technologies"
- **The importance of protecting "critical technology"**
  - We live in a growing world of "critical technology"
  - Increase in threats involving "critical technology"
  - Commercial interests and "critical technology"
- **How are governments and businesses managing and protecting "critical technology"?**

Session Topics and Speakers

Controls on Intangible Transfers of Technology (ITT) **Mr. Robert Shaw**, Program Director for Export Control and Nonproliferation, James Martin Center for Nonproliferation Studies (CNS), Middlebury Institute of International Studies at Monterey (MIIS)

Cybersecurity Standards for Managing Critical Technology **Dr. Ian Stewart**, Executive Director Washington DC Office, James Martin Center for Non-proliferation Studies (CNS)

Foreign Investment Controls and Critical Technology**, Mr. Ryan L. Cathie**, Senior Research Fellow, Center for Policy Research (CPR) at the University at Albany, State University New York (SUNY)

Critical Technology Protection Best Practices by Industry, **Mr. George Tan**, Principal, Global Trade Security Consulting Pte Ltd, Singapore

Controls on Intangible Transfers of Technology (ITT), Robert Shaw, CNS/MIIS

1. **The heightened focus on critical technologies, and particularly emerging technologies, is increasing the priority and importance of ITT and its management.**

2. **Definition(s) of Intangible Transfer of Technology (ITT)**

3. **Trends that are increasing the priority/importance of ITT controls -- particularly for industry**

Cybersecurity Standards for Managing Critical Technology, Dr. Ian Stewart, CNS/MIIS

1. **The imperative of addressing cybersecurity of export-controlled information**
2. **Some concepts and key terms that export control practitioners should become with**
3. **Considerations around how to approach the question of cybersecurity of export-controlled information**
4. **The question of how to prevent misuse of controlled and uncontrolled but sensitive software by actors of concern**

Foreign Investment Controls and Critical Technology,

Ryan Lynch Cathie, CPR/UAlbany/SUNY

1. Overview of FDI Controls
2. Approaches to FDI Controls
3. Changing Scope of FDI Controls

Overview of Foreign Investment Controls

- Foreign Direct Investment (FDI) brings capital and technology to a country and governments around the globe have an interest in high levels of FDI
- There have been an increasing number of mergers & acquisitions (M&A) and FDI in recent years, particularly in technology start-ups across the globe
- In recent years, many governments have increasingly viewed FDI through a national security lens and have sought to protect industries dealing in defense, dual-use, and “critical technologies”
- According to the OECD, up to 60% of global direct investment is subject to investment controls

Risks Posed by FDI

- **FDI can increase vulnerability to IP infringement, trade secret appropriation, or forced and unauthorized technology transfers**
  - FDI and corporate acquisitions can blur the line between voluntary and forced technology transfers
  - FDI in domestic companies by entities affiliated with the government can be motivated by strategic reasons (desire to acquire advanced technology or IP) rather than commercial interests

Approaches to FDI Controls

- **Valuation or ownership percentage thresholds will trigger a mandatory filing requirement**
- **Different thresholds may apply to different types of foreign investors**
  - State-owned or state-controlled investor vs. non-foreign government investor
- **Different thresholds may apply to different types of businesses (e.g. defense vs. agriculture)**

Trends in Foreign Investment Controls

1) In recent years, an increasing number of countries have adopted FDI review regimes or expanded the scope of their existing FDI controls

2) COVID-19 and Russia's invasion of Ukraine have accelerated and amplified calls for expanded FDI controls

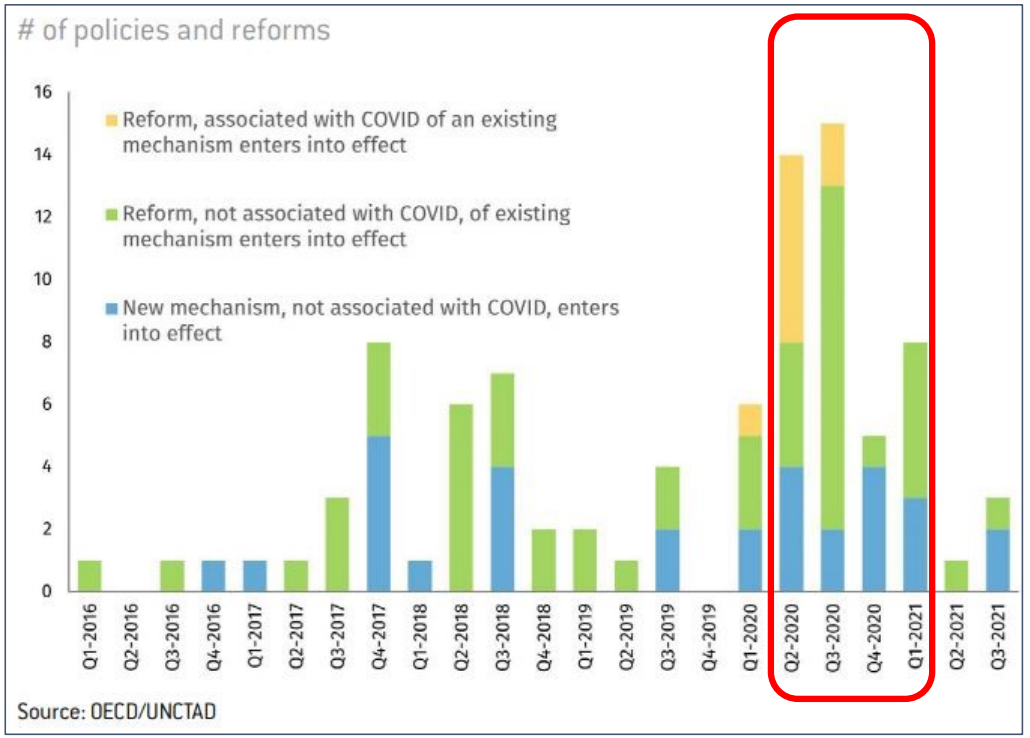
3) Lowering of thresholds that trigger FDI authorization requirements

4) National security concerns moving to the forefront and countries are requiring investment screening for a broader range of industries – focus on safeguarding "critical technologies"

5) Less focus on the nationality of the investor and more emphasis on affiliations (e.g. state-controlled)

Expanded FDI Regimes

- Japan, Korea, India, China, the U.S., France, UK, Germany, Italy, Spain, Australia, and New Zealand have expanded the scope of their FDI review regimes in the past 3 years
- COVID-19 exposed a need for investment controls due to a lack of PPE and medical devices and fears of predatory investments
- Movement has been further amplified by the Russian conflict in Ukraine



Lowering Review Thresholds

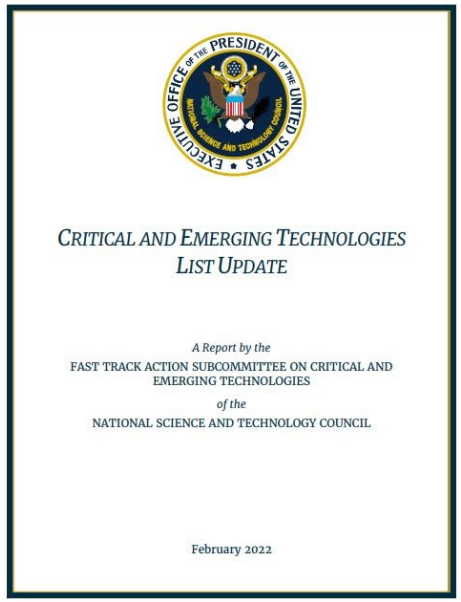
Most countries with investment controls in place review investments and acquisitions involving voting shares of between 10% and 25%

- **Japan** may require examinations of acquisitions involving shares of 1% or more since 2019
- **Australia** lowered the approval threshold for "national security businesses" to 10% or more in 2021
- **France** lowered the threshold for screening non-EU investments to 10% or more in 2021
- **Italy** introduced notification requirements for EU investors in sensitive sectors and non-EU investors acquiring 10% or more of entities deemed to be "strategic"

Screening a Broader Range of Sectors

Countries are adding critical technology sectors to mandatory FDI reviews

- **Korea** - introduced changes to the *Foreign Investment Promotion Act* to allow intensified screening of investment in sectors considered to pose a high threat for leakage of core national technologies as defined by the *Act on the Prevention of Divulgence and Protection of Industrial Technology*
- **Japan** – in May 2020, Japan tightened investment screening regulations on additional industry sectors including nuclear energy, telecommunications, software, integrated circuits, and medical devices
- **United States** - the Foreign Investment Risk Review Modernization Act (FIRRMA) and the Export Control Reform Act (ECRA) of 2018 added 27 "critical technologies" requiring mandatory filing with the Committee on Foreign Investment in the United States (CFIUS) for investments in these designated industries



EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

CRITICAL AND EMERGING TECHNOLOGIES LIST UPDATE

A Report by the

FAST TRACK ACTION SUBCOMMITTEE ON CRITICAL AND EMERGING TECHNOLOGIES

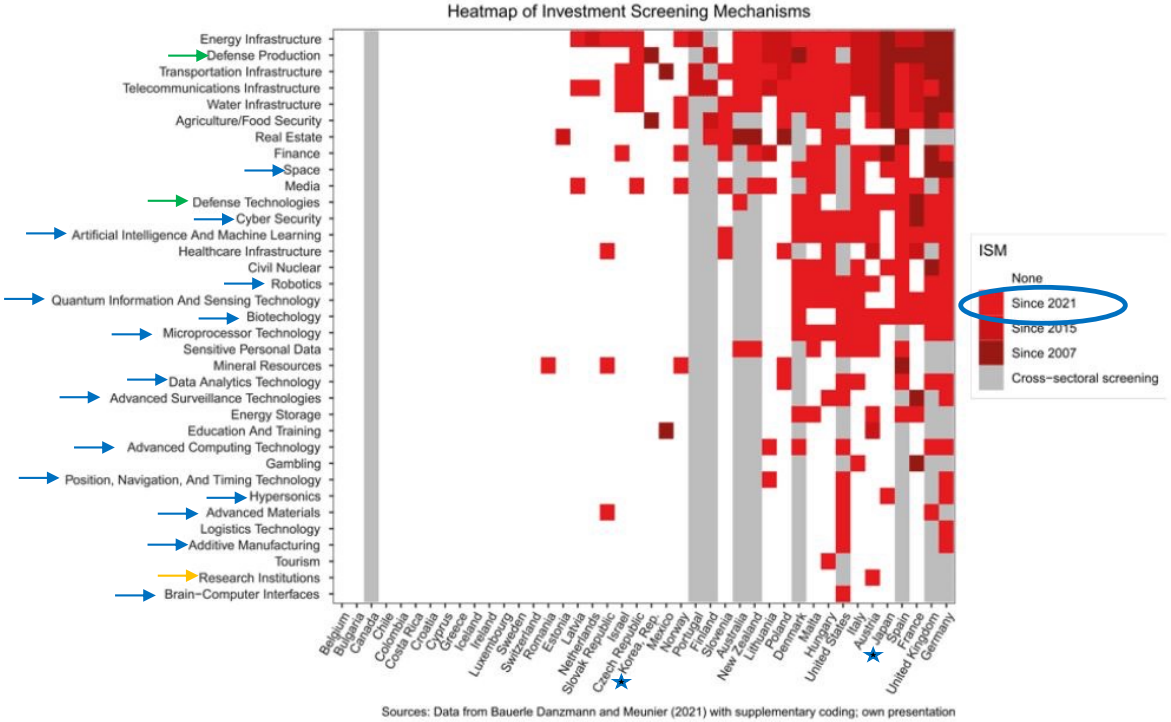
of the

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

February 2022

EXAMPLE: Sectors with FDI Controls in OECD Countries

G 11: Sectors with investment controls in OECD countries in 2007, 2015 and 2021



Sources: Data from Bauerle Danzmann and Meunier (2021) with supplementary coding; own presentation

Emphasis on Affiliations

The fact of whether an investor is considered state-owned / state-controlled is a critical factor in the assessment of national security implications related to FDI

- The **EU Commission** warned in 2019 that the rate of acquisitions involving state-owned investors from certain countries had increased rapidly and encouraged Member States to develop FDI screening mechanisms
- **Spain -** requires any investment made by a company that is considered to be controlled by the government, whether directly or indirectly, to undergo mandatory screening
- **Australia -** applies specific screening obligations to “foreign government investors”
- **India -** amended the FDI Policy in April 2020 with Press Note 3, which introduced intensified FDI screening procedures for investment originating in neighboring countries

More Changes on the Horizon?

- **Greater convergence/integration between export and FDI controls**
  - In the U.S., the Foreign Investment Risk Review Modernization Act (FIRRMA) and Export Control Reform Act (ECRA) of 2018 were linked to protect technological edge and prevent adversaries gaining access to advanced and next generation technologies from U.S. companies
- **Establishment of bilateral and multilateral agreements that enable countries with like-minded values to mutually waive investment controls (in specified sectors)**
- **Increased "outbound" investment screening**
  - Korea's *Act on the Prevention of Divulgence and Protection of Industrial Technology* established the Industrial Technology Protection Committee, which is empowered to block outbound investment by firms that hold "national core technology" developed by government subsidies for R&D
  - U.S. is also considering outbound investment controls in the form of the National Critical Capabilities Defense Act (NCCDA), which would impose restrictions related to outbound investment in certain industries deemed a part of "national critical capabilities" or destined for "countries of concern"

Implications for Businesses in Southeast Asia

- An increasing number of countries maintain foreign investment controls on critical technology
- The expansion of global FDI regimes can complicate cross border transactions and necessitates more effective due diligence on the part of industry
- Companies dealing in critical technologies must carefully assess the affiliations of all potential investors and business partners and work to effectively safeguard critical technologies

Critical Technology Protection Best Practices – Industry Perspective, George Tan, GTSC Pte Ltd.

1. **Where is "Critical Technology?**
2. **Why "Critical Technology" Needs Protection?**
3. **What are "Critical Technology" Protection Best Practices by Industry?**

Where is Critical Technology

Where can you find Critical Technology (apart from defense and military related)

1) **Company Technology** means all Technology used in or necessary for the conduct of the business of the Company or any of its Subsidiaries, or owned or held for use by the Company or any of its Subsidiaries

2) **Licensed Technology** means the Licensed Patents and the Licensed Know-How. Project IP means the Intellectual Property

3) **Joint Technology** means the Joint Know-How and the Joint Patent Rights

Why needs Protection

1) Crown Jewels of a Company
2) Reputation – Corporate Citizen
3) Partnership / Trust Worthy Company
4) Trade Secret / Know-How
5) Patent / IP / Trade Mark
6) Defence Strategies → **Commercial Usage**
7) National Security & Regional Security

What are the Best Practices

1) Robust Internal Compliance Program – in particular Classification, Screening, Storage, Access and Transfer
2) Technology Control Plan (TCP – mini ICP for Technology)
3) Comprehensive Risk Assessment Mechanism – in particular Infrastructure, HR and Record Keeping
4) Cyber Security
5) Data Access Management
6) Compliant Culture – company-wide effort
7) Export Control Community

Critical Technology Protection Best Practices Q&A

Thank you for your time and attention!

We welcome your questions and comments!