Regional Digital Trade Integration Index (RDTII)

Lecture 6

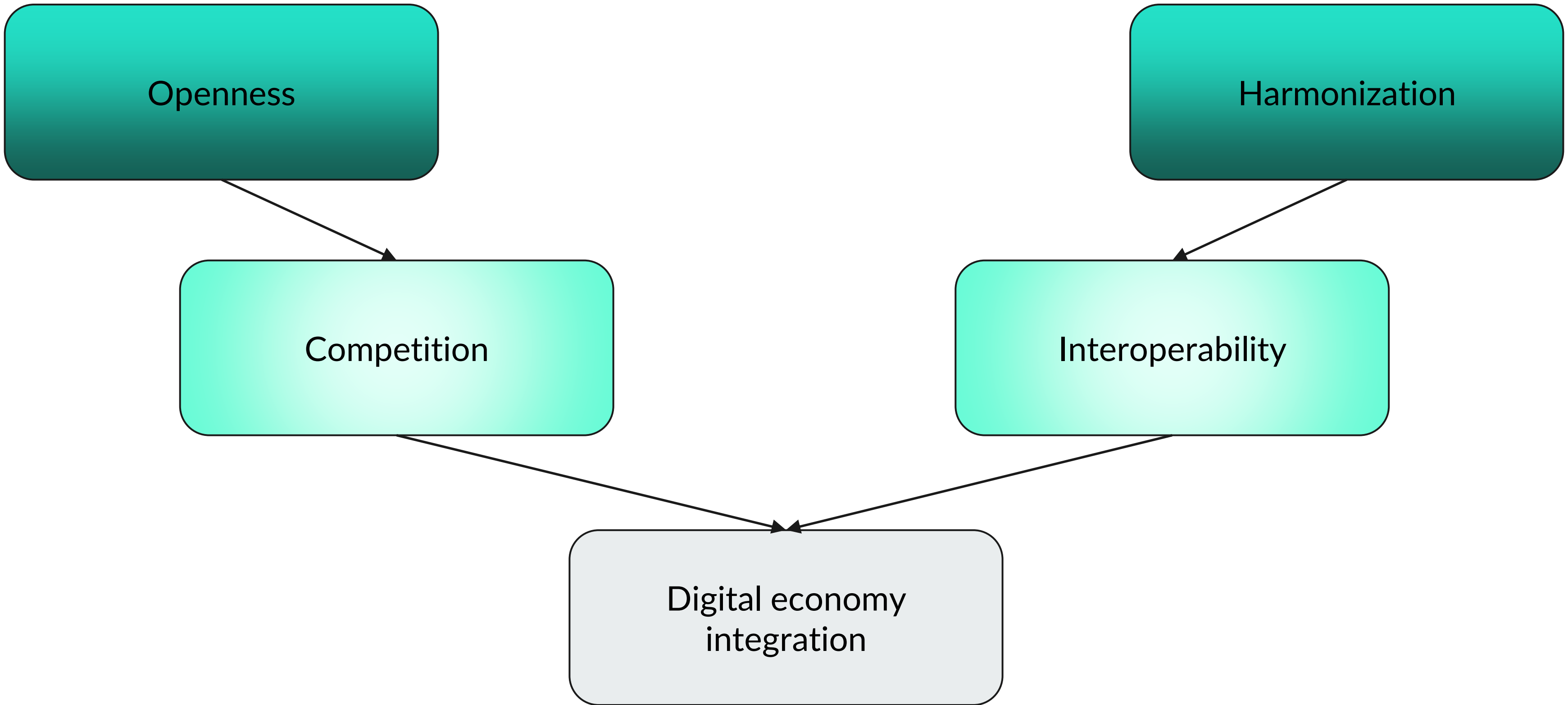
Overview

- Recapitulation of RDTII and Scoring Results
- RDTII Exercises & Answer

What is “digital trade”?

- Trade in tangible goods through e-commerce
- Trade in digital content (e.g., media content)
- Trade in online services
- Cross-border investment in digital-trade infrastructure (e.g., telecommunications)

Why on openness and harmonization of digital trade regulation



How does RDTII capture openness and harmonization ?

11 Pillars → **44 Sub-pillars**

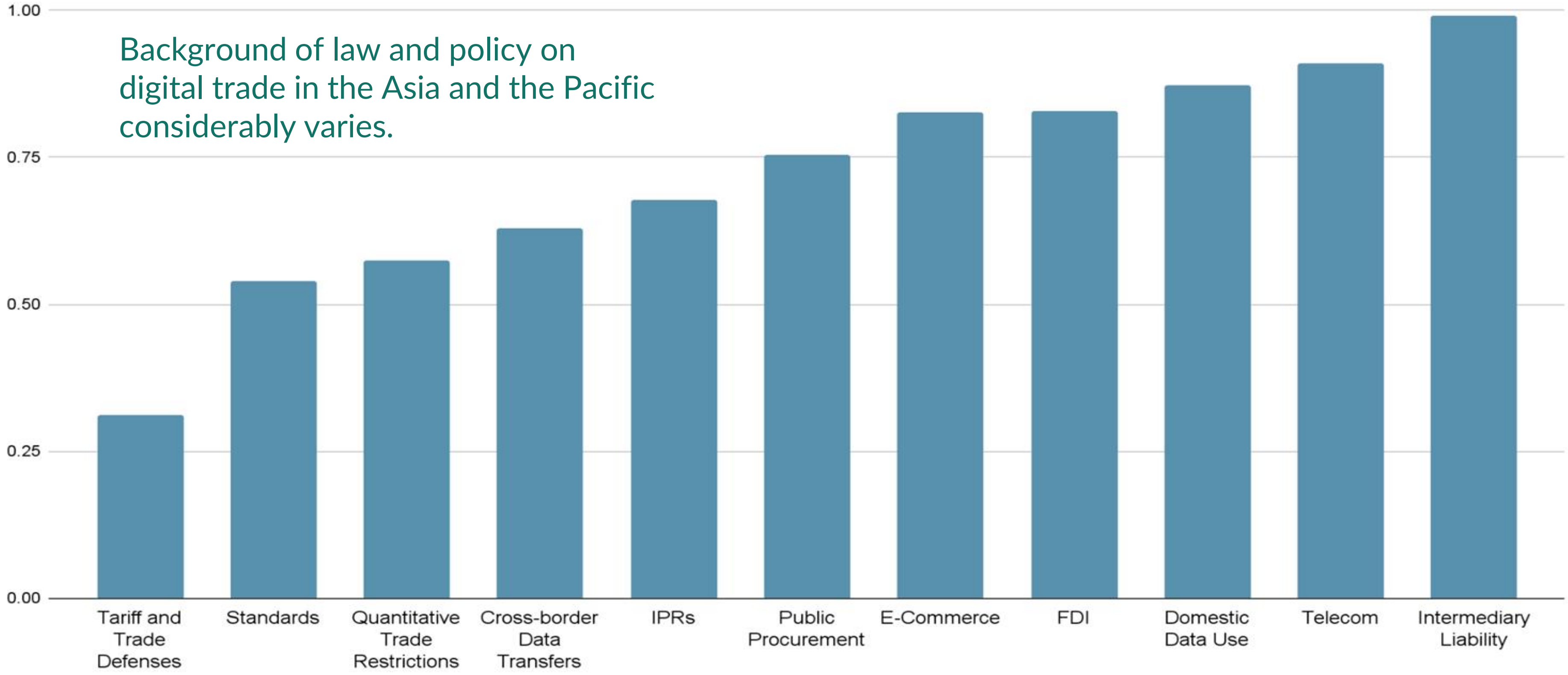
RDTII is a proxy only for digital economy integration in terms of the openness and harmonization. RDTII *does not* engage in a subtle balancing of other policy objectives.

For some pillars, this degree is represented by additional costs regulation creates.

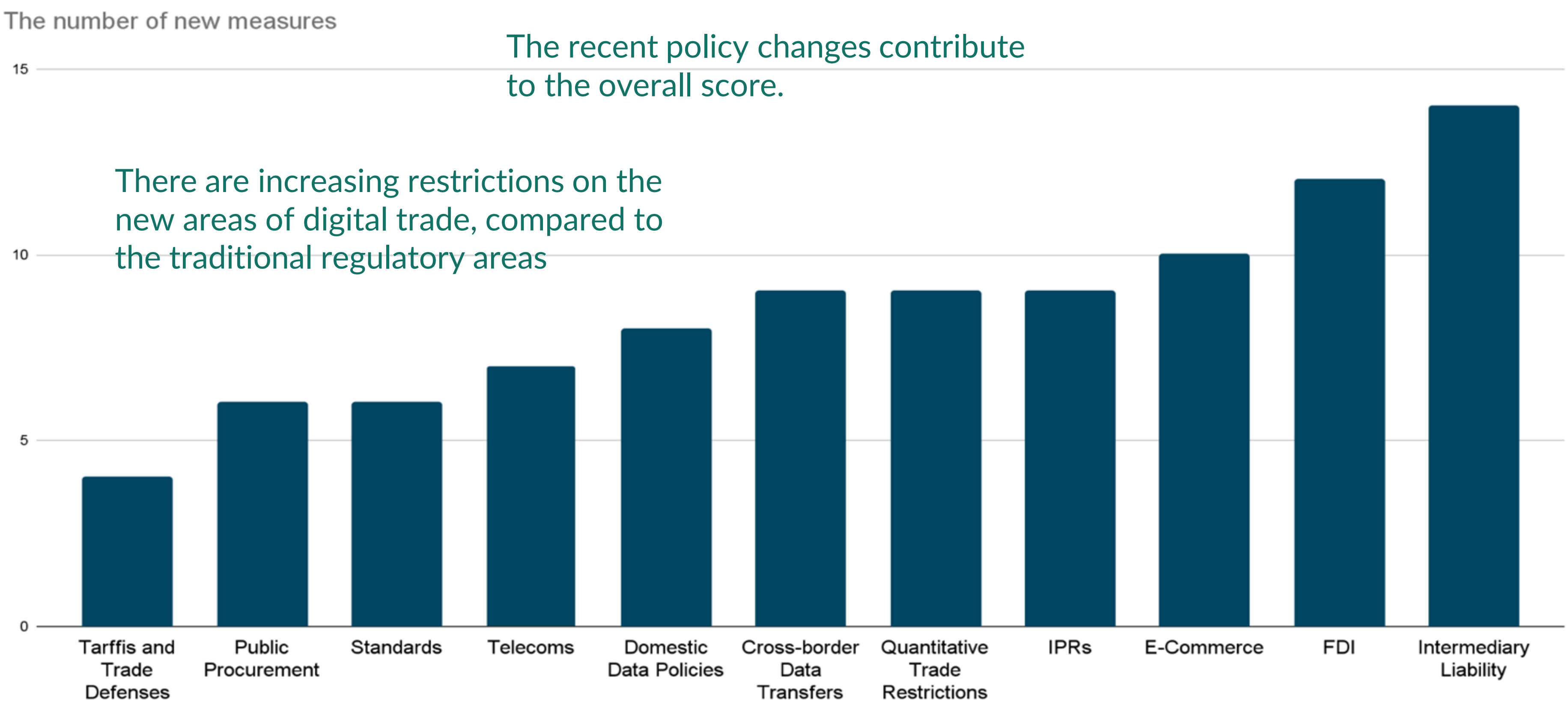
For other pillars, the consideration of openness and harmonization is multi-faceted. The RDTII helps policymakers to make a more informed decisions on complex digital-trade policy issues.

RDTII pillar-by-pillar scores

Background of law and policy on digital trade in the Asia and the Pacific considerably varies.



The number of recent policy changes



RDTII Exercises & Answers

Exercise 1: Tariffs and Trade Defence on ICT-related Goods

Explain why the RDTII considers whether an economy is a member of ITA I and II, which mandates elimination duties on ICT products, even though the RDTII already covers coverage ratio of zero-tariff lines on ICT products.

Being a signatory to the WTO ITA I and its expansion, an economy is bound to eliminate import duties on the covered products. Investors and traders would benefit from the improved market access, predictability and certainty.

Common themes: international legal frameworks; certainty and predictability

Exercise 2: Public Procurement Related to ICT Goods and Online Services

The following measures are restrictions on source codes, encryption, and trade secrets. Categorize the following measures into two groups. Which of the groups has the greater potential to restrict digital trade?

1. Indonesia requires that providers of custom-made software must provide or escrow the source codes associated with their service.
2. The Republic of Korea requires that suppliers of certain software, network, and hardware equipment submit the source code of their products to pass “the Cryptographic Module Validation Process.”
3. The Philippines requires technology and knowledge transfer to the procuring entity for the provision of consulting services.
4. India prescribes certain modes or methods for encryption for e-government and e-commerce procurement.
5. The Republic of Korea requires suppliers of software, network, and hardware equipment that deals with “non-confidential but important information” to comply with encryption standards developed in the Republic of Korea (e.g., ARIA, SEED, LEA, and Hight).

Exercise 2: Public Procurement Related to ICT Goods and Online Services

The following measures are restrictions on source codes, encryption, and trade secrets. Categorize the following measures into two groups. Which of the groups has the greater potential to restrict digital trade?

1. The Republic of Korea requires that suppliers of certain software, network, and hardware equipment submit the source code of their products to pass "the Cryptographic Module Validation Process." **A requirement to submit source codes**

Common themes: varying degree of openness (blocking vs. discouraging)

2. The Philippines requires technology and knowledge transfer to the procuring entity for the provision of consulting services. **A requirement to submit source codes**
3. India prescribes certain modes or methods for encryption for e-government and e-commerce procurement. **A requirement to use a specific encryption standard**
4. The Republic of Korea requires suppliers of software, network, and hardware equipment that deals with "non-confidential but important information" to comply with encryption standards developed in the Republic of Korea (e.g., ARIA, SEED, LEA, and Hight). **A requirement to use a specific encryption standard**

Exercise 3: Foreign Direct Investment in Sectors Relevant to Digital Trade

The second sub-pillar covers joint venture requirements in sectors relevant to digital trade. Explain why it is restrictive to require a foreign firm to form a joint venture with a domestic firm.

Forming a joint venture with a domestic firm may not be proper in given circumstances in which the foreign firm is situated. Furthermore, there is concern that technology might be forcefully transferred.

Common theme: the government may not be the best decision-maker

Exercise 4: Intellectual Property Rights

The most common two copyright exceptions are the doctrine of fair use and the doctrine of fair dealing. Which one is more conducive to international digital trade, i.e., favorable to foreign businesses venturing into a domestic market? Explain why.

The doctrine of fair use is a flexible case-by-case test such that it creates more room for new and innovative use of the a copyrighted work, rather than limiting permissible uses to enumerated items as the fair dealing does.

Common theme: narrow policy choice

Exercise 5: Telecommunications Infrastructure and Competition

The first sub-pillar looks at the degree to which the telecommunication market is liberalized. This sub-pillar is designed to measure the openness for competition in the market. By your own terms, define the "liberalization" of a telecom market.

RDTII considers "liberalization" in telecom market in light of three factors:

- The extent to which the telcom-facility sector has been regulated under **competition rules**
- The extent to which **access networks** or '**the last mile**' are owned by dominant players in the market
- The extent to which **foreign ownership** in telecom facilities is allowed

Common theme: mindful of lack of transparency

Exercise 6: Cross-Border Data Policies

The first sub-pillar deals with local storage, processing, and infrastructure. Categorize the following measures into one of the three types of conditions on cross-border data policies.

1. Turkey requires system operators, payment institutions and electronic money institutions to collect all relevant documents and records within the country.
2. Viet Nam requires foreign providers of internet services and telecommunications to store in Viet Nam personal data of their users.
3. Australia requires companies to both store and process health records, excluding personal information within Australia.
4. The Republic of Korea requires financial service providers that use cloud services to locally process credit and unique identification information of their users.
5. Indonesia requires foreign banks and payment networks to establish a local data center to process electronic transactions.

Exercise 6: Cross-Border Data Policies

The first sub-pillar deals with local storage, processing, and infrastructure. Categorize the following measures into one of the three types of conditions on cross-border data policies.

Common theme: differentiation of types of data (personal and non-personal) (e.g., Pillar 7)

1. Turkey requires system operators, payment institutions and electronic money institutions to collect all relevant documents and records within the country. Local storage
2. Viet Nam requires foreign providers of internet services and telecommunications to store in Viet Nam personal data of their users. Local storage
3. Australia requires companies to both store and process health records, excluding personal information within Australia. Local processing
4. The Republic of Korea requires financial service providers that use cloud services to locally process credit and unique identification information of their users. Local processing
5. Indonesia requires foreign banks and payment networks to establish a local data center to process electronic transactions. Local infrastructure

Exercise 7: Domestic Data Policies

The second sub-pillar deals with data retention requirements. Which one of the following data retention requirements do you think deserves a higher score (more restrictive) in this sub-pillar?

1. Australia requires a telecommunication service provider to keep specific telecommunications data relating to the services it offers for two years at least (the data include the subscriber and the accounts of telecommunications devices, the source of a communication, the destination of a communication, the date, time and duration of a communication, the type of a communication, and the location of equipment or a line used).
2. The Republic of Korea requires data controllers to destroy personal information upon the fulfilment of the purpose of processing the information

Common theme: the government may not be the best decision-maker

Exercise 8: Intermediary Liability and Content Access

The first sub-pillar deals with safe-harbor provisions for internet intermediaries. Economies that do not have any safe-harbor provisions for the intermediaries receive a high score (restrictive). Explain why the lack of safe-harbor provisions restricts digital trade, if they do.

The lack of safe-harbor restricts digital trade because the internet Intermediaries are not the most efficient cost bearers and discourages digital trade due to less certainty and chilling effect of potential litigation.

Common theme: the lack of measures is restrictive

Exercise 9: Quantitative Trade Restrictions

The first sub-pillar deals with (import) bans on ICT products and online services. Write one example of recent import bans imposed by any economy on ICT products or online services of foreign businesses.

Answer:

-Few Arab states have a ban on Voice over internet protocol (VoIP), which prohibits the use of audio and video calls using Whatsapp, Facetime, etc.

-United States ban on Huawei products

Exercise 10: Technical Standards Applied to ICT Goods and Online Services

The third sub-pillar deals with an additional screening or testing requirement on ICT imports for the interest of national security. Which one of the following is the least restrictive towards digital trade?

1. New Zealand requires companies that use a 5G network equipment to receive approval under security assessment by the Government Communications Security Bureau to prevent national security threats.
2. India requires in-country security testing on all telecom network equipment and products.
3. The Russian Federation requires equipment and devices containing encryption to be registered with the Federal Security Service (FSS) and the manufacturer or the seller to obtain FSS notification upon importation or exportation of such equipment. Notification of the FSS is a prerequisite for the import into the territory of the Eurasian Economic Union (EAEU), or export from the territory of the EAEU of equipment containing encryption elements.
4. Thailand requires telecommunication equipment to be tested to ensure that the products conform with the technical standard prescribed by the national agency. The agency recognizes both local and foreign testing laboratory results which conform to the required conditions.

Common theme: harmonization and interoperability

Exercise 11: Online Sales and Transactions

The first sub-pillar deals restrictions to online purchases, delivery of online purchases and online advertising. which one of the following measures do you think is the most restrictive towards trade in e-commerce?

1. The Philippines ban foreign ownership of retail trade enterprises with paid-up capital of less than USD 2.5 million.
2. India provides that B2B e-commerce must not have more than one vendor that accounts for more than 25% of sales.
3. Pakistan prohibits the broadcast of advertisements produced in India or featuring Indian actors and characters.

Common theme: trade-blocking

Report on Regional Digital Trade Integration Index Guidelines (RDTII), please visit https://www.unescap.org/kp/RDTII

Thank you.