BANCA D'ITALIA
EUROSISTEMA

The Digital Economy Amid Rising International Tensions

Roma, 24 October 2025

Cybersecurity and Trade Fragmentation

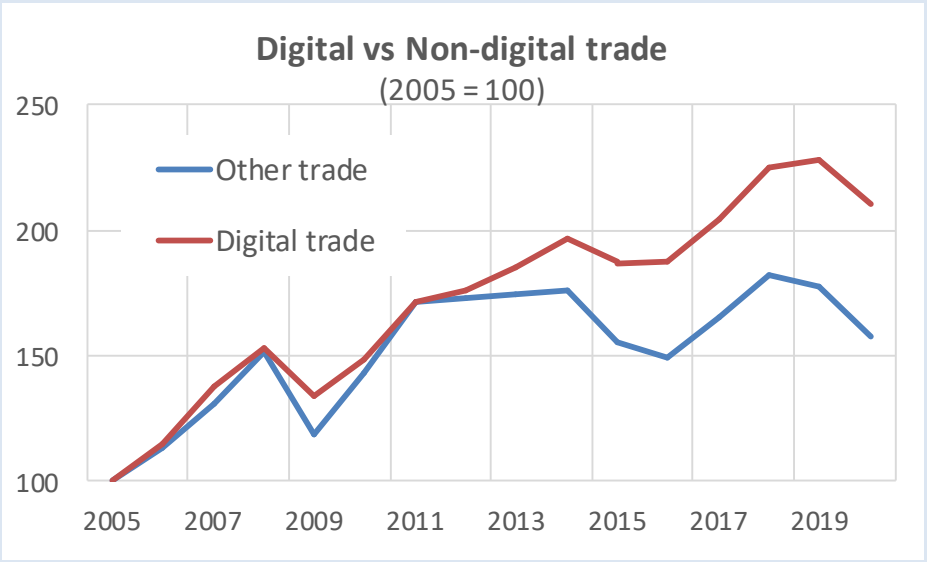
By Lorenzo Bencivelli

Plan of the talk

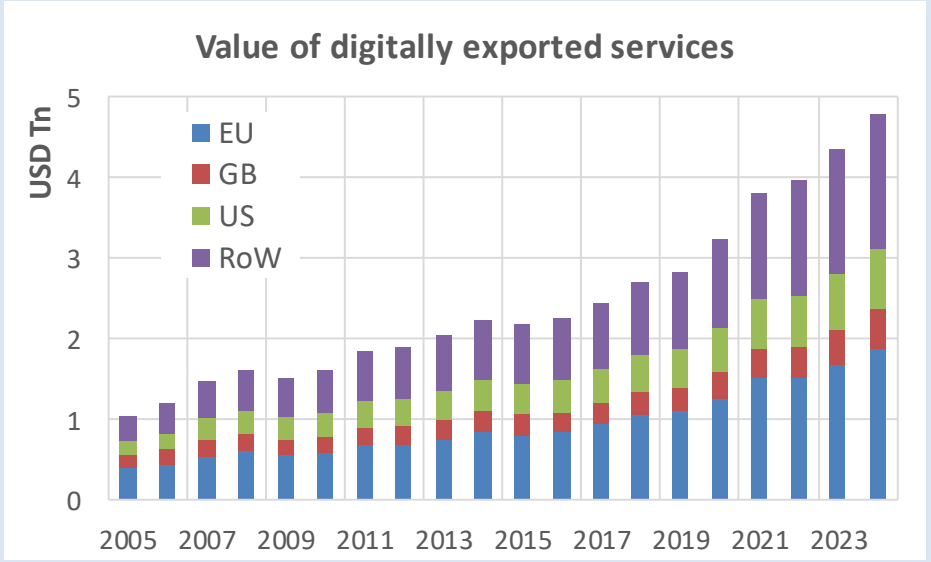
- Introduction
- Cybersecurity as a non-tariff barrier
- Impact on trade and corporates' operation
- Geopolitical dynamics and regulatory divergence
- Conclusions

Introduction

Introduction – some major trends in global trade



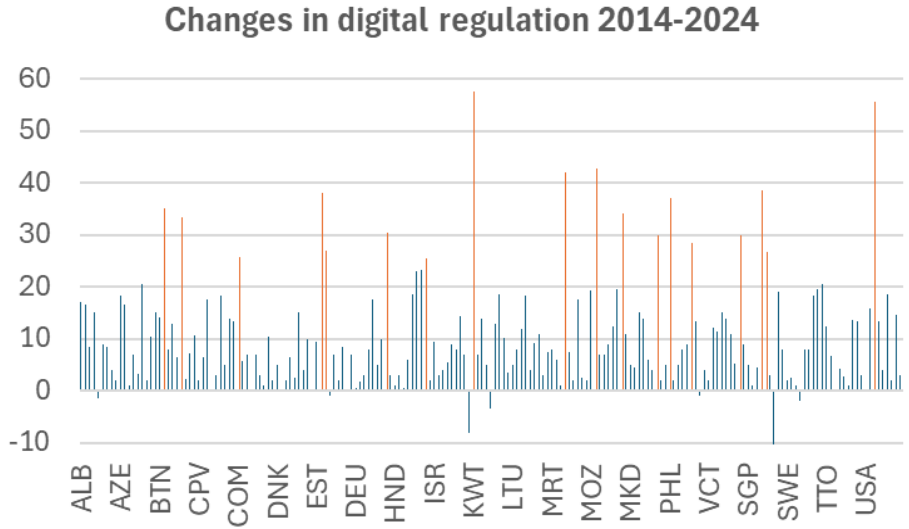
Source: OECD calculation on TiVa.



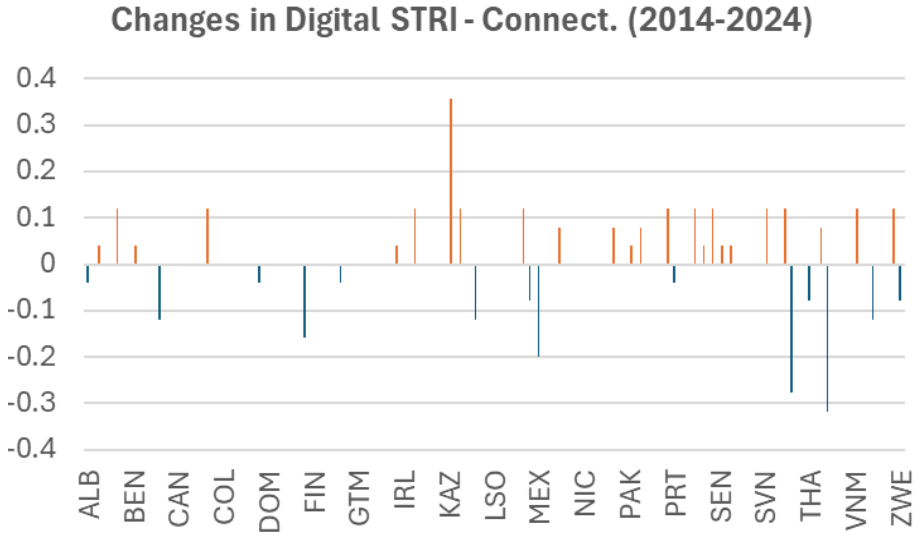
Source: WTO.

- Digital trade in goods and services has has outgrown non-digital trade
- Service sector benefitted particularly from the increase in digital technologies
- Baldwin (2025): while trade in goods seems to have peaked, service trade is still growing

Introduction – regulation in the digital domain has increased



Source: ITU-ICT Regulatory Tracker.



Source: ITU-ICT Regulatory Tracker.

- **The digital world has become a much more regulated** space, especially among emerging markets
- **Higher regulation comes along with higher restrictions** to digital trade

Cybersecurity as a non-tariff trade barrier

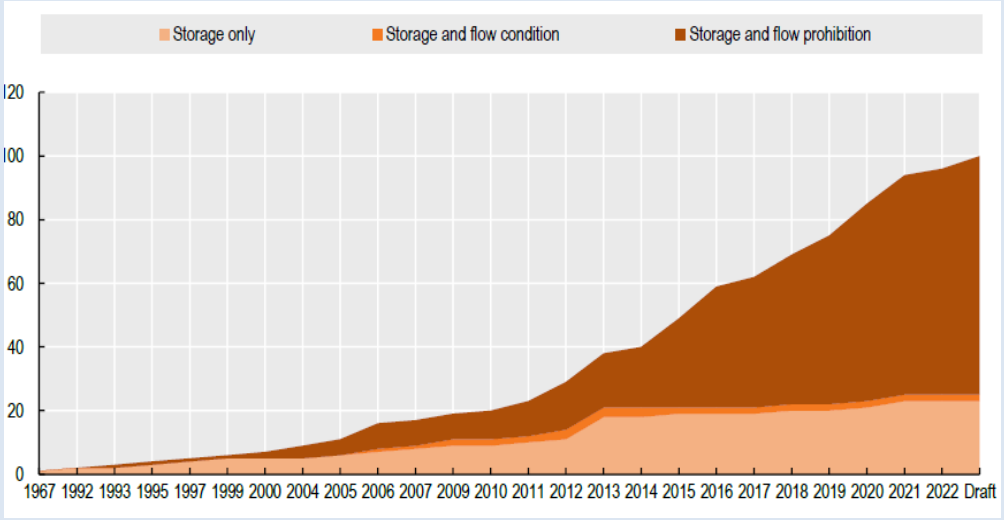
Cybersecurity as non-tariff trade barrier – a conceptual fmw

BANCA D'ITALIA
EUROSISTEMA

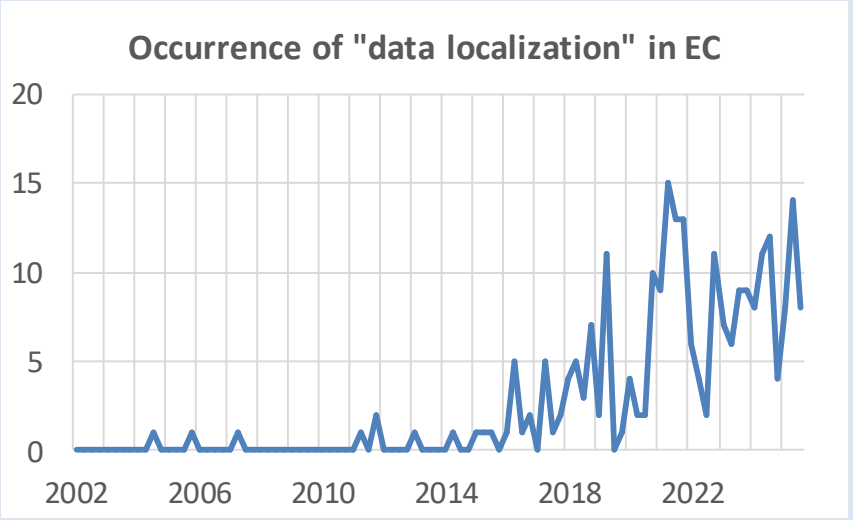
While aimed at protecting national infrastructure and consumer data, cybersec measures often function as NTBs (especially for services). Four mechanisms contribute to this dynamic:

- **Data localization laws** – By requiring data to be stored or processed within national borders and restricting cross-border flows they hinder the scalability of digital services
- **Divergent cybersecurity standards** – Non-interoperable standards increase compliance costs, create asymmetries in market access and forces MNCs to segregate the ICT systems
- **Security driven restrictions** – Affecting foreign digital infrastructure providers (e.g., cloud) can act as de facto protectionist tools, fragmenting global value chains
- **Ambiguities in WTO and other FTA** - Rules regarding cybersecurity exceptions often allow for broad interpretations legitimizing restrictions under the guise of national security

Data localization laws



Source: Del Giovane et al (2023) OECD PP No. 278.



Source: NL Analytics.

- Data localization laws are swiftly increasing over time
- *"The position paper is critical of policies that risk creating 'two separate systems' […] need for many companies to create distinct policies and procedures when dealing with China compared to the rest of the world…"*

Data localization laws

Source: Global Data Alliance.

Diverging cyber security standards

Fragmented Cybersecurity Regulations – Multinational companies face complex, overlapping regulations with inconsistent language and enforcement across countries.

Operational Inefficiencies and Risks – Segregating IT systems by country increases costs and risk of non-compliance due to regulatory divergence.

Compliance Complexity and Costs – Companies must comply with multiple standards like NIST, ISO, and GDPR, raising administrative burdens and costs.

Challenges in Harmonization – Efforts to standardize regulations, face political, cultural, and institutional obstacles worldwide.

Source: Marotta and Madnick (2020,2021).

Cybersecurity and FTAs

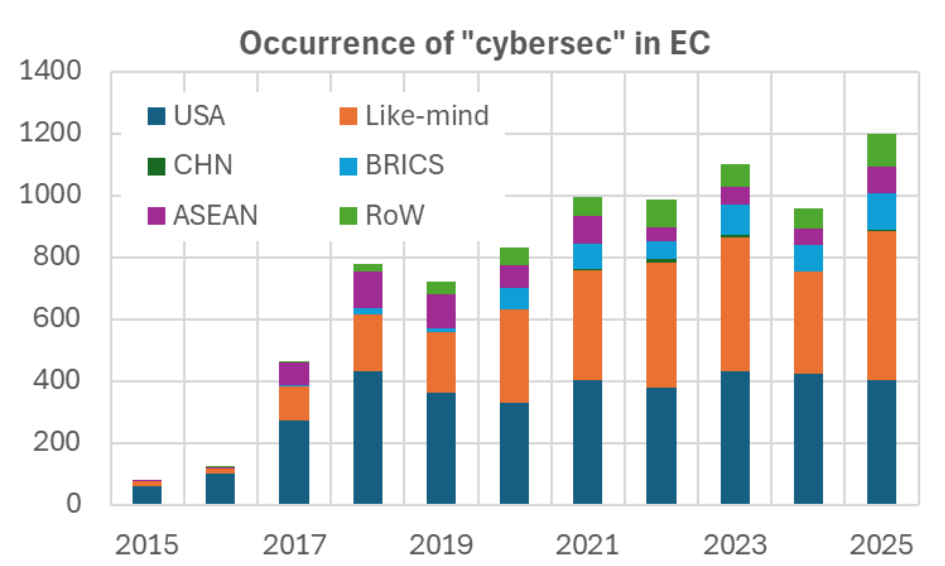
- **Cybersecurity as a Trade Policy** - Cybersecurity concerns are treated as national security priorities. These measures **blur the line between legitimate security regulation and protectionism**

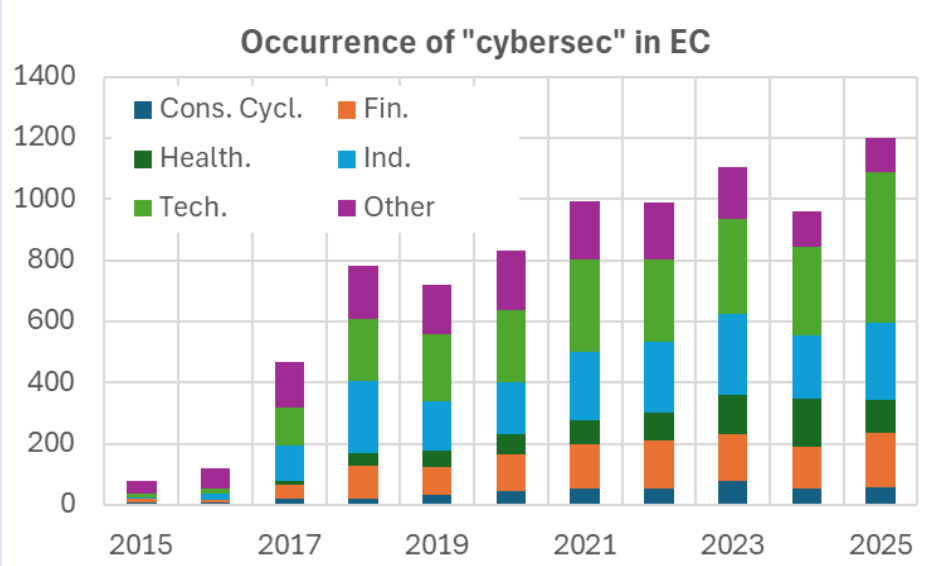
- **The WTO legal framework** - GATT, GATS, and TRIPS allows members to deviate from liberalization commitments for actions "necessary to protect essential security interests." **There is a case for "self-judging"** clause creating legal ambiguity

- **New digital trade agreements** - While attempting to discipline the matter, these agreements **allow exceptions when justified by "legitimate public policy objectives"** mirroring WTO's open-ended security clauses

Impact on trade and Multinational Corporations (MNCs) operations

Impact on MNCs operations

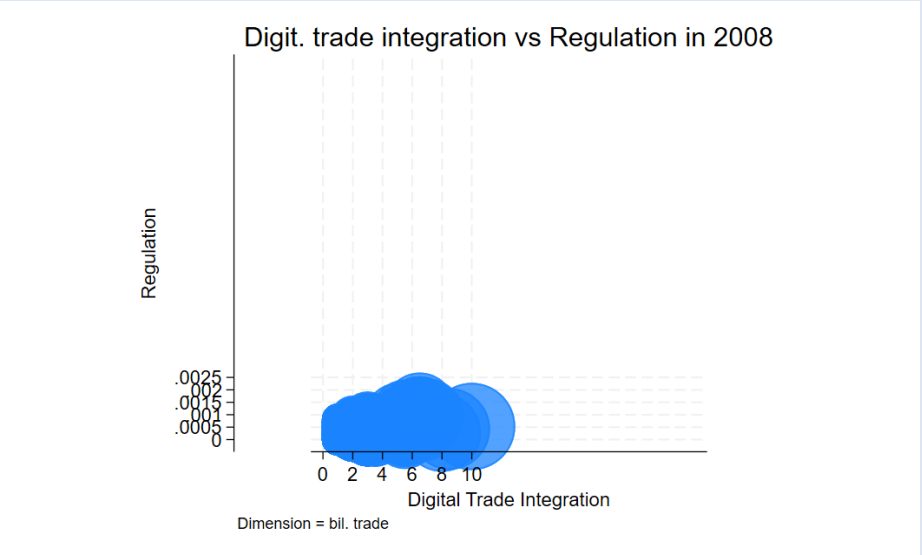


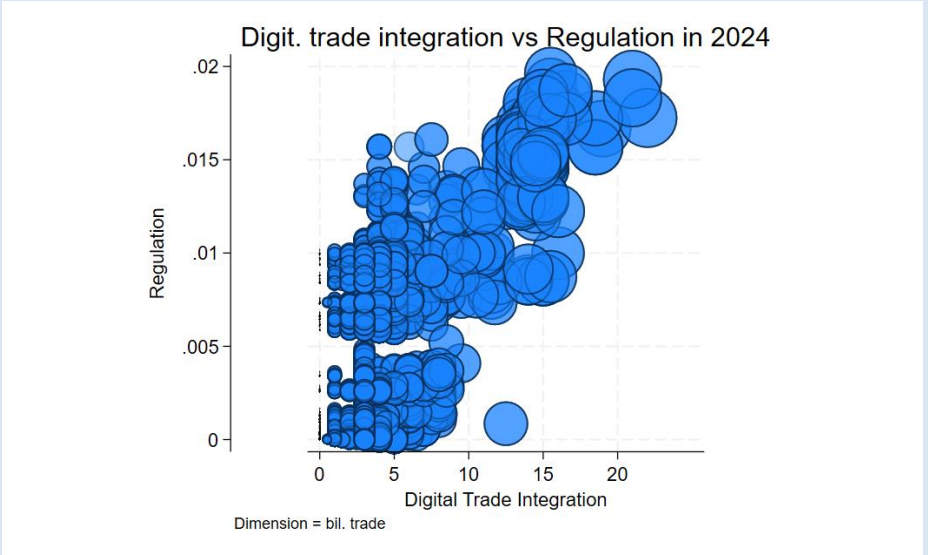


Source: NL Analytics.

- Among listed corporates, "cybersecurity" **matters for earnings starting from 2017**
- As a concern, is **mostly shared among firms in the US and likeminded** (EU,CA,UK, CH …)
- **Technology, industry and finance** are the most affected sectors

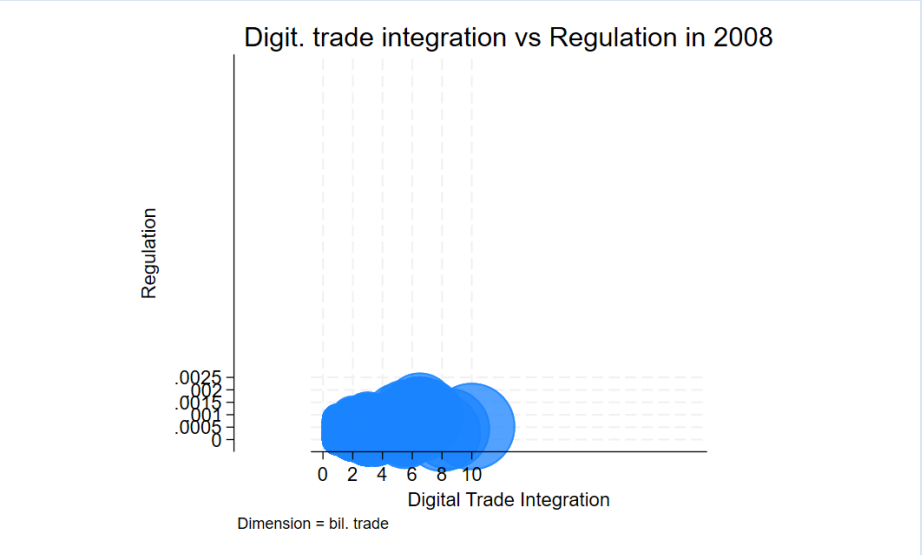
Impact on trade – Digital trade integration

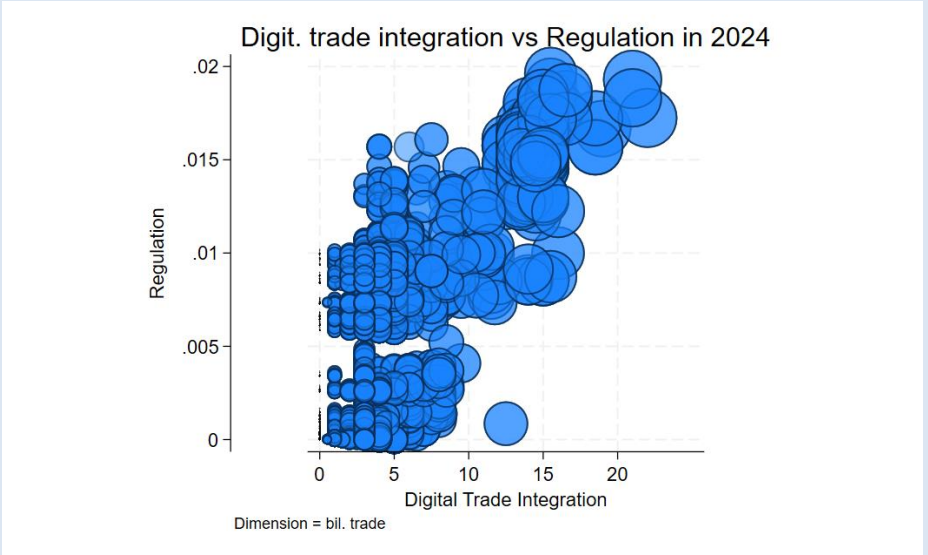




- To grasp the comprehensiveness of cyber regulation we will use **INDIGO** (**Index of Digital Trade Integration and Openness**), a OECD's integrated database
- **INDIGO Bilateral is the subset of the OECD INDIGO database that focuses specifically on bilateral trade flows** in services between reporting and partner countries.

Impact on trade – Digital trade integration





- From 2008 to 2024, **digital trade integration and regulatory intensity have increased**, suggesting that digital interconnectedness was accompanied by stronger regulation
- However, the heterogeneity in regulatory intensity across countries points to growing **risks of regulatory fragmentation**

Impact on trade – A model to evaluate the impact on trade

BANCA D'ITALIA
EUROSISTEMA

- **We will use a simple economic model that predicts trade between two countries** based on their size (GDP) and distance - like gravity

- **The model explains most trade patterns**, so we can see the extra impact of digital integration (INDIGO) and cybersecurity on trade.

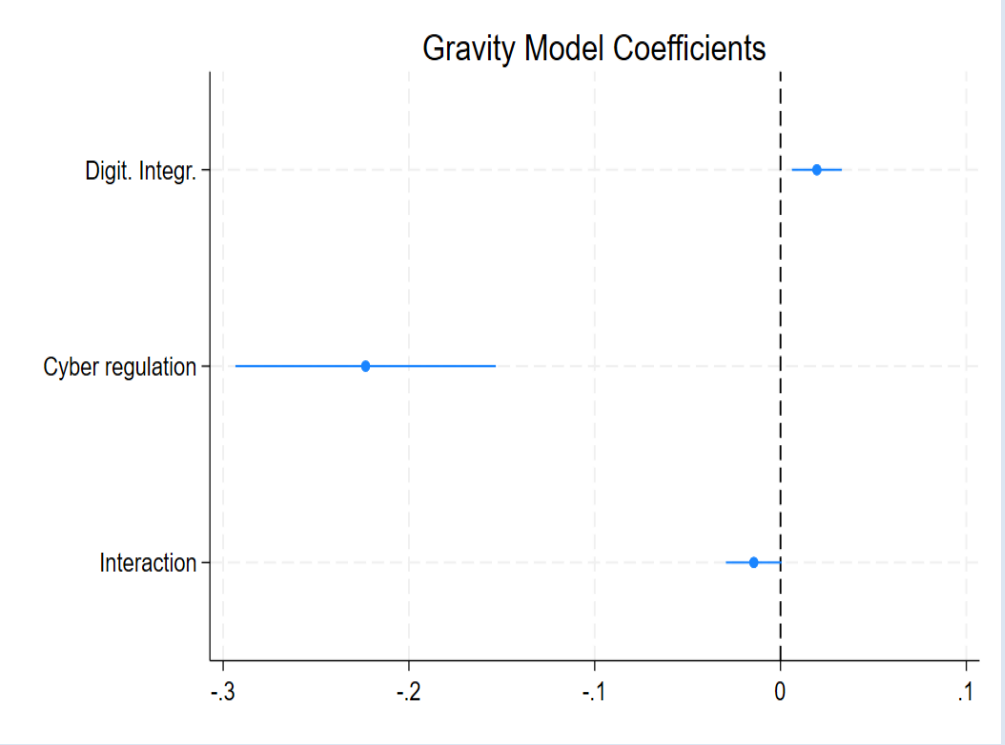
- We **combine trade data with country characteristics** (GDP, distance, geography, population, agreements …) **and digital indicators**. The model estimates how each factor changes bilateral trade flows

- The hypothesis we're testing is that **what matters for bilateral trade is not only the level of regulation in each country but also the integration of the two regulatory framework**

Impact on trade – A model to evaluate the impact on trade

BANCA D'ITALIA
EUROSISTEMA

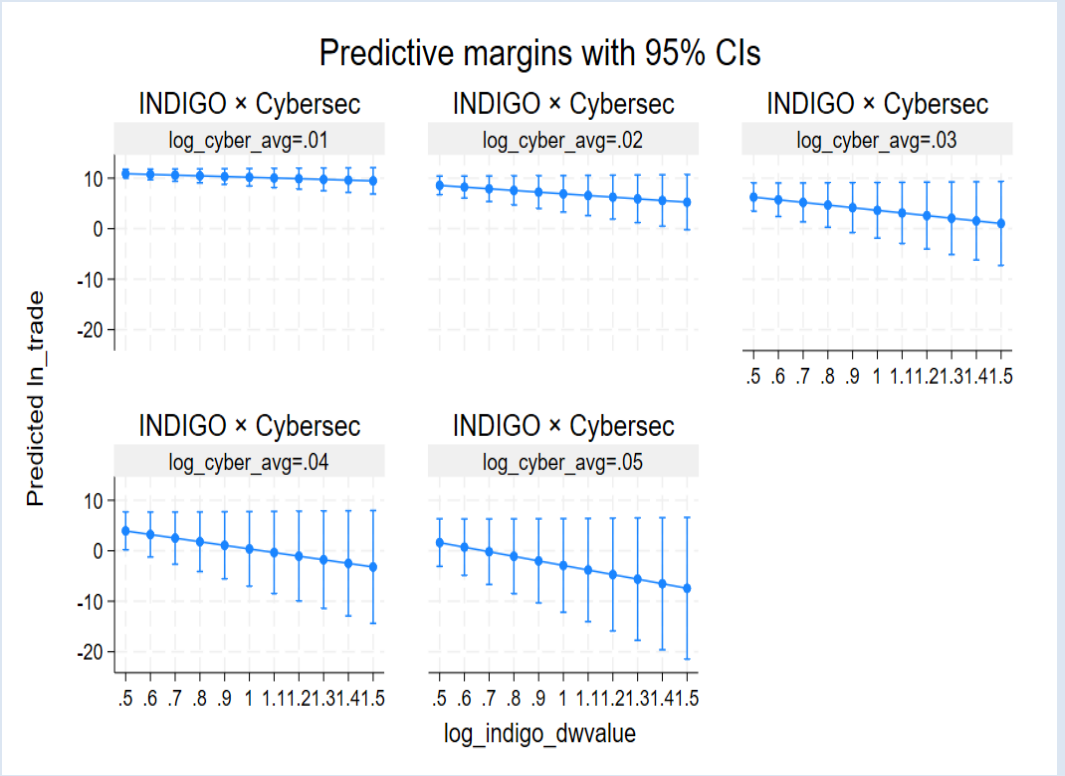
- **Digital integration** agreements have a small positive effect on trade flows (endogeneity)
- **Tighter cybersecurity regulations** are associated with a negative impact on trade, possibly due to compliance costs and data restrictions
- **The interaction** term suggests that digital agreements mitigate some negative effects of strict cybersecurity rules.



Impact on trade – A model to evaluate the impact on trade

BANCA D'ITALIA
EUROSISTEMA

- Trade benefits from digital integration **decrease as cybersecurity requirements become stricter**
- At **low cybersecurity restrictiveness, digital integration supports trade**
- The effect shrinks as cyber regulations is being tightened



Geopolitical dynamics and regulatory divergence

Regulatory divergence – The state of the art

BANCA D'ITALIA
EUROSISTEMA

The current regulatory frameworks of the three major trading blocks reflect their respective core values leaving little room to negotiate a possible enhanced integration

Jurisdiction	Sovereignty Model	Free Flow of Data	Ban on Data Localization	Regulatory Focus
USA	**Firm Sovereignty**	✓ **Yes**	✓ **Yes**	Commercial freedom, privacy as consumer right
China	**State Sovereignty**	✗ **No**	✗ **No**	National security, centralized control
EU	**Individual Sovereignty**	✓ **Yes***	✓ **Yes***	Privacy as a fundamental right (GDPR)

Source: Gao (2002).

Geopolitical trajectory – Heading toward splinternet?

BANCA D'ITALIA
EUROSISTEMA

- **Geopolitical Polarization:**
  - EU and China locked in a "**digital limbo**": dialogue exists, but trust deficit persists
  - **US–China rivalry accelerates bifurcation** of standards (AI, 5G, data governance)

- **EU's Strategic Shift:**
  - European Defence Readiness 2030 and Preparedness Union Strategy sees **cybersecurity as core of security policy**
  - **Push for resilience**, AI regulation, and supply chain security

- **Future Outlook:**
  - **Risk of a Digital Cold War** with competing blocs
  - **Possible emergence of regional digital compacts** (e.g., EU–Japan, DEPA)
  - **Firms face rising compliance costs** and need for multi-regime strategies

Source: Vanberghen (2025a, 2025b) and Stallkamp (2021).

Conclusion

Conclusion

- **Cybersecurity will be a ground for economic diplomacy in the foreseeable future**
  - Notwithstanding the significant effort to integrate it into trade agreements, the room to "weaponize" is wide

- **MNCs may end up caught in the cross-fire**
  - Compliance costs and the possibility of web segregation may limit considerably the extent of their operations and innovation capability

- **Trade gains from higher integration in the cyber domain, possibly offsetting some of the extra costs arising from diverging cyber regulation frameworks**

- **Perspectives for enhanced cooperation in cyber domain are all but bright**

THANK YOU FOR YOUR ATTENTION

lorenzo.bencivelli@bancaditalia.it