Council of the European Union
General Secretariat

Brussels, 03 June 2025

WK 7283/2025 INIT

LIMITE

TELECOM

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Rethinking the EU's digital security: building autonomy through partnerships - Presentation

Delegations will find in the annex the presentation "Rethinking the EU's digital security: building autonomy through partnerships"

euiss European Union Institute for Security Studies

PUBLIC

Rethinking EU's Digital Security: Building Autonomy through Partnerships

[redacted] – *Senior Policy Analyst, Cyber and Digital Technologies*

[redacted] – *Project Officer, Cyber Diplomacy and International Partnerships*

The EUISS is an agency of the European Union

Agenda

About the European Union Institute for Security Studies

- Publications
- Events
- Projects

Rethinking the EU's Digital Security: Building Autonomy Through Partnerships

- Autonomy as a means to improve digital security
- Building “strategic digital autonomy”: A two-fronts ambition
- The EU’s potential partnerships

About the European Union Institute for Security Studies

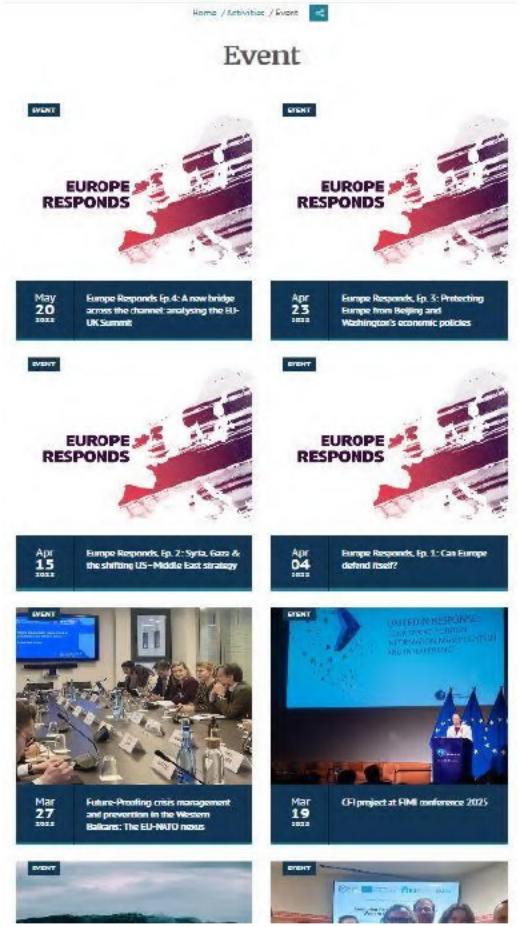
About us

The European Union Institute for Security Studies (EUISS) is the Union's Agency analysing foreign, security and defence policy issues. Its core mission is to assist the EU and its member states in the implementation of the Common Foreign and Security Policy (CFSP), including the Common Security and Defence Policy (CSDP) as well as other external action of the Union.

The Institute was set up in January 2002 as an autonomous agency under Council Joint Action 2001/554 [now regulated by Council Decision 2014/75/CFSP] to strengthen the EU's analysis, foresight, and networking capacity in external action. The Institute also acts as an interface between the EU institutions and external experts – including security actors – to develop the EU's strategic thinking. The EUISS is now an integral part of the structures that underpin the further development of the CFSP/CSDP.

Publications

- Briefs
- Chaillot Papers
- Commentaries
- Reports
- Books



euiss

Events

- Europe Responds Series
- Conferences
- Roundtables
- Dialogues
- Exercises

Projects

- **EU Cyber Direct – EU Cyber Diplomacy Initiative (EU CD)**
- **Advancing the Cyber Programme of Action (PoA)**
- **Countering Foreign Interference (CFI)**
- **Chips Diplomacy Support Initiative (CHIPDIPLO)**
- **SCOPE**

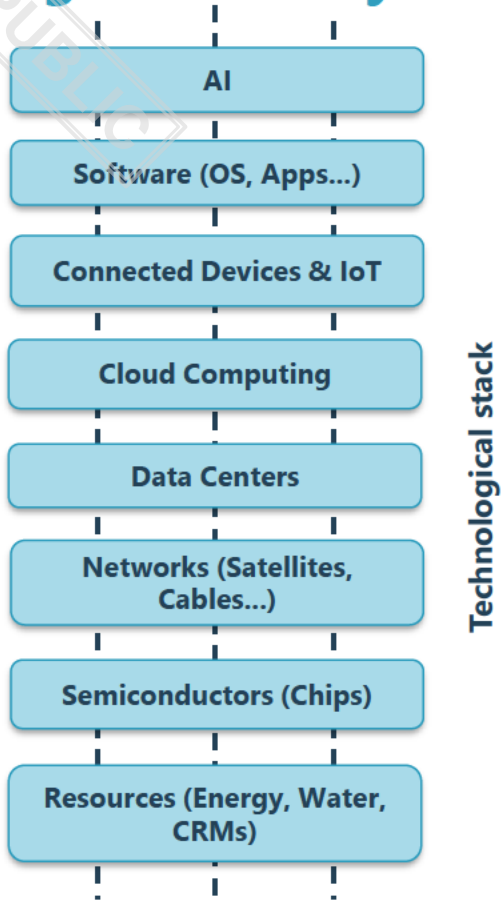
ACCESS OUR PUBLICATIONS

SCAN ME

Rethinking the EU's Digital Security: Building Autonomy Through Partnerships

Autonomy as a means to improve digital security

From data security to digital security:



Autonomy as a means to improve digital security

The weaponization of dependencies:

- **Globalization / Globalized tech supply chains**

→ E.g., Different layers of the digital stack are developed across multiple regions, creating complex interdependence.

- **Dependencies created through niche and/or oligopolies**

→ E.g, Strategic chokepoints emerge where production is concentrated (like Taiwan's dominance in semiconductors, and lithography machines).

- **A strategic asset for one can be a systemic vulnerability for the other**

→ E.g, Microsoft revoking access of the Chief Prosecutor of the ICCs to his emails.

> The EU seeks greater autonomy – the freedom to decide and act - to limit external coercion. This ambition took shape in 2019-2020 in the European discourses through the project of "digital sovereignty."

Building “Strategic Digital Autonomy”: A Two-Front Initiative

Three levers of “Digital Sovereignty”

- **Supporting Research & Development and Innovation:**
  → Allows Europe to shape next-gen tech — embedding democratic values (e.g., transparency, data portability) and gaining strategic advantage via patents and standards.

- **Strengthening the regional digital and technological industrial base:**
  → Reduces reliance on foreign providers by scaling domestic and regional solutions across critical sectors.

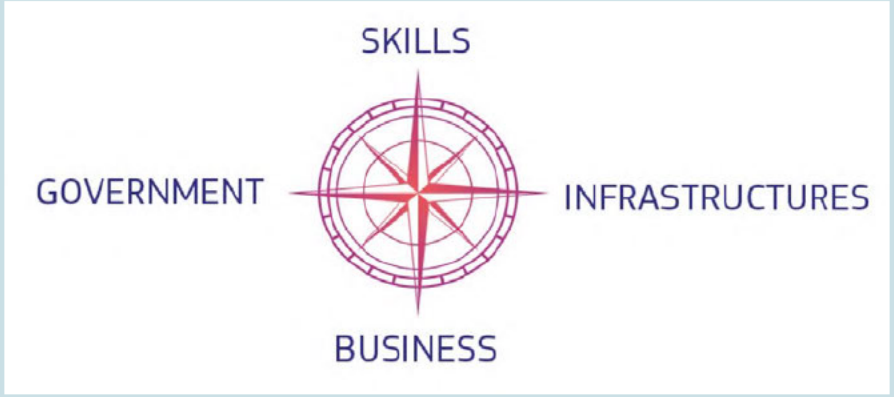
- **Enforcing Norms and Regulation:**
  → Laws like the GDPR, DSA, DMA, and AI Act, and certifications like the upcoming EUCS enable Europe to regain control over digital infrastructure and data flows.

Building Strategic Autonomy: A Two-Front Initiative

Developing European Capabilities

Internally

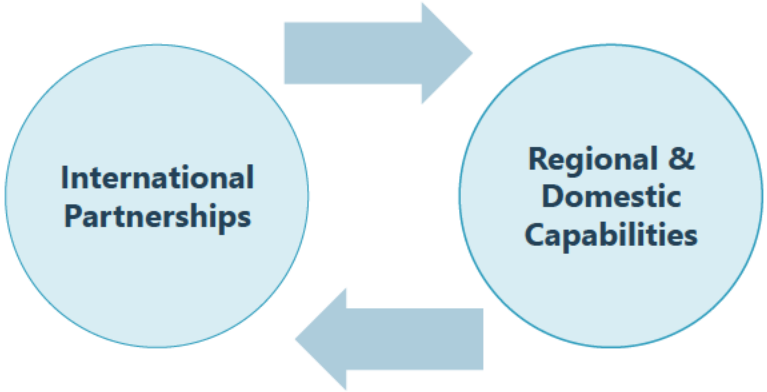
European Digital Compass



Source: European Commission

Externally

Developing European Capabilities through International Partnerships



The EU's Potential Partnerships

Different Types of Partnerships

Like-minded countries	Countries with Dynamic Tech Ecosystem	Critical and Emerging Regions
Partners that broadly share the EU's democratic values, regulatory approaches, and commitment to an open, rules-based digital order.	Partners with fast-growing digital sectors or emerging tech leadership, which may not fully align with the EU on values but represent key trade or innovation opportunities.	Partners that are rapidly developing digital capacity and seeking partnerships, particularly in areas like infrastructure, digital skills, or governance.
Japan, South Korea, Australia, United Kingdom, Canada, United States…	*India, United Arab Emirates, Saudi Arabia, China…*	*Africa (UA), Indo-Pacific, Ukraine, Eastern Neighbourhood…*

Key Takeaways

Digital security is more than cybersecurity

Digital sovereignty must be pursued through the development of internal capabilities and external partnerships

Strategic clarity, not fragmentation

To assert itself in the global technological race and to safeguard its interests in an unstable geopolitical context, the EU must continue to align its digital strategies to develop a systemic approach that considers the entire technological stack and acknowledges the complementarity of internal (regional capabilities) and external (partnerships) dimensions in strengthening 'digital sovereignty'.