



**Interregional cooperation is key to identifying solutions and moving towards a more integrated cyber security market**

#### PROJECT FEATURES



**Implementation period:**

June 2018 – May 2023



**Funding:**

€ 1.53 M ERDF



**Twitter account:**

@CyberEurope



**Website:**

[www.intereurope.eu/cyber](http://www.intereurope.eu/cyber)



European Union  
European Regional  
Development Fund

#### Three major barriers encumbering the interregional cooperation within the European Union have been identified:

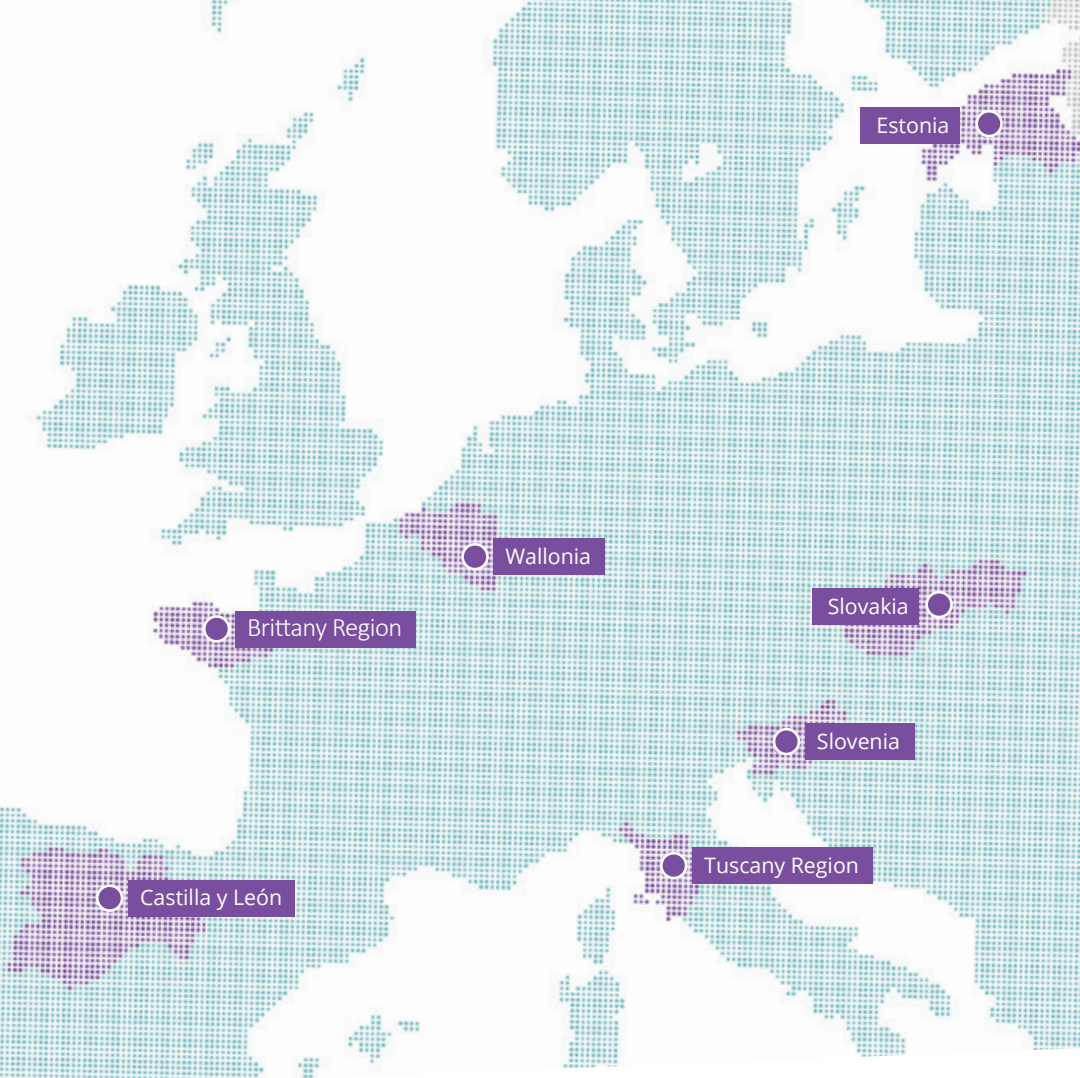
- Lack of coordination between relevant actors
- Market fragmentation
- Lack of skills

**Interreg Europe CYBER aims to boost the competitiveness of the European cyber security SMEs and to create synergies among the European cyber security valleys.**

#### The project focuses on developing regional action plans with clear policy instruments to effectively bolster interregional cooperation:

**June 2018 - May 2021:** Phase 1 is dedicated to Interregional learning based on the exchange of experience among partner regions. Together with their regional stakeholders, partner organisations (1) analyse territorial needs, (2) identify, exchange and investigate good practices, (3) develop action plans to improve regional policies.

**June 2021 - May 2023:** Phase 2 is dedicated to the implementation and monitoring of regional Action Plans based on the lessons learnt thanks to the interregional exchange during the Phase 1.



**Project partners**

**Lead Partner:**

Bretagne Development Innovation (France)

**Partners:**

Digital Wallonia (Belgium)

Tuscany Region (Italy)

Institute for Business Competitiveness of Castilla y León (Spain)

Chamber of Commerce and Industry of Slovenia (Slovenia)

Brittany Region (France)

Estonian Information System Authority (Estonia)

Kosice IT Valley (Slovakia)

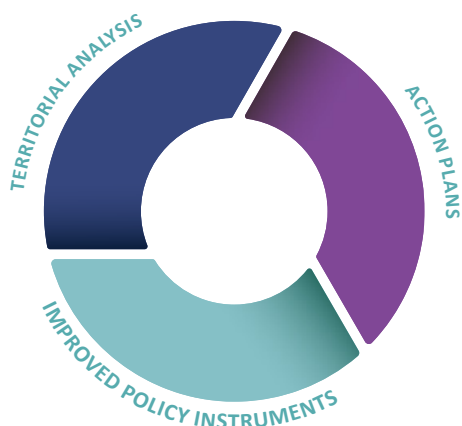
**Advisory Partner:**

European Cyber Security Organisation (ECSO)

The EU market is valued at EUR 25 billion and has a very diverse industry landscape, made of 12 000 companies of which 74 % are micro companies and SMEs.

A series of interregional events are organized to connect stakeholders from European regions and to share the best policy practices.

**INTERREGIONAL LEARNING**



- Territorial Analysis: Identifying needs and exchanging good practices
- Action Plans: Supporting regional authorities in boosting the competitiveness of the local cybersecurity SMEs
- Improved Policy Instruments: Monitoring the implementation and providing recommendations

Due to their privileged connection with the local ecosystems, the EU regions are playing a fundamental role in structuring the still young European cyber security ecosystem

- Regions are important part of the triple helix model of economic development, which involves governments, academia and business.
- Regions facilitate the development of the local cyber security ecosystems by involving RTOs, training centres, services operators, incubators, SMEs and established large companies.
- Regional level is significant in disseminating good practices and establishing preventive measures and immediate response services due to its proximity with the end-users.
- Regions play key role in addressing cyber security skills shortage, as the demand for cyber security providers and operators are increasing at the EU local level.
- Due to the potential cyber attacks, local public administrations are the direct users of cyber security products when developing their sectoral policies (e.g. health, energy or transport).



Regione Toscana