EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER

The role of the regions in strengthening the European Union's cyber security

WG4 | Support to SMEs, coordination with countries and regions

March 2019

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the official partner to the European Commission in implementing the contractual Public-Private Partnership (cPPP) on cyber security. ECSO unites a great variety of the European cyber security stakeholders, including large companies, SMEs and startups, research centres, universities, end-users, operators, clusters and associations, as well as the local, regional and national administrations across the European Union (EU) Member States, the European Free Trade Association (EFTA) and H2020 Programme associated countries. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg4_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

EXECUTIVE SUMMARY

Uniquely positioned, the European regions hold a privileged connection to their local ecosystem. To reach global awareness and competitive innovation in cyber security, regional authorities have a structured cooperation with their local end-users, critical industries and services, competitive and innovative SMEs, cutting edge R&D labs and training centres.

The European Union cyber security landscape will be shaped by initiatives having a direct impact on regional ecosystems such as the European Cybersecurity Centre and Network, the European digital innovation hubs and renewed smart specialization strategy in each region.

The European Cyber Security Organisation (ECSO) considers the inter-regional cooperation as a game changer in structuring the European cyber security landscape.

The added-value of the regional engagement for cyber security is highlighted through key examples of existing regional initiatives and related policy and financial tools.

— Strategic planning & decision making: Regions elaborate their own economic and innovation strategy, which is known as Smart Specialisation Strategy (S3).

— Long-term investor & supporter of the "Made in Europe": Regions are the managing authority for the European Structural and Investment Funds (ESIF).

— The Triple Helix System: Regions host a triple helix system offering a truthful environment for innovation to the market.

— Proximity with end-users & critical infrastructures: Regions are accessible territories of experimentation and connection with end-users.

— Reducing cyber security skills shortage: By supervising education and training, regional authorities play a key role in addressing cyber security skills shortage.

AUTHORS: Annie Audic, Project Director "Continuum Training, Research, Innovation", Brittany Regional Council Brittany Region; Chair, **ECSO Working Group 4** dedicated to support SMEs and regional cooperation.

Contributions of experts from 11 European regions, including **Basque country, Brittany, Castilla y León, Central Finland, Cyprus, Kosice, Greater Region of Luxembourg, North Rhine Westphalia, Paris Region, Upper Austria, Wales, Wallonia.**

Danilo D'Elia, Senior Policy Manager & Ana-Isabel Llacayo, Policy Manager, **ECSO Secretariat**

TABLE OF CONTENTS

Connecting European Cybersecurity Smart Regions Map iv

1. Introduction 5

2. Why Do "Smart Territories" and Regional-Level Practices Matter? 6

2.1. Critical challenges to the European cyber security market 6

2.2. Successful regional frameworks and mechanisms for innovative and competitive cyber security ecosystems 7

3. ECSO as a Laboratory of Innovative Ideas and Exchange, and Implementation of the Best Practices with Regions 14

4. Post-2020 Cyber Security Landscape for Regions 15

5. Regions Play a Catalyst Role in Europe's Cyber Security 17

Appendix – "Smart Territories" in Cyber Security: Success Stories 18

1.Basque Country, Spain 19

2. Brittany, France 20

3. Castilla y León, Spain 21

4. Central Finland, Finland 22

5. Luxembourg and the Greater Region 23

6. Bochum and the Metropolis Ruhr, North Rhine-Westphalia, Germany 24

7. Paris Region, France 25

8. Wallonia, Belgium 26

CONNECTING EUROPEAN CYBERSECURITY SMART REGIONS

CYBER
Interreg Europe

An interregional cooperation project to enhance public policies for the competitiveness of cybersecurity companies

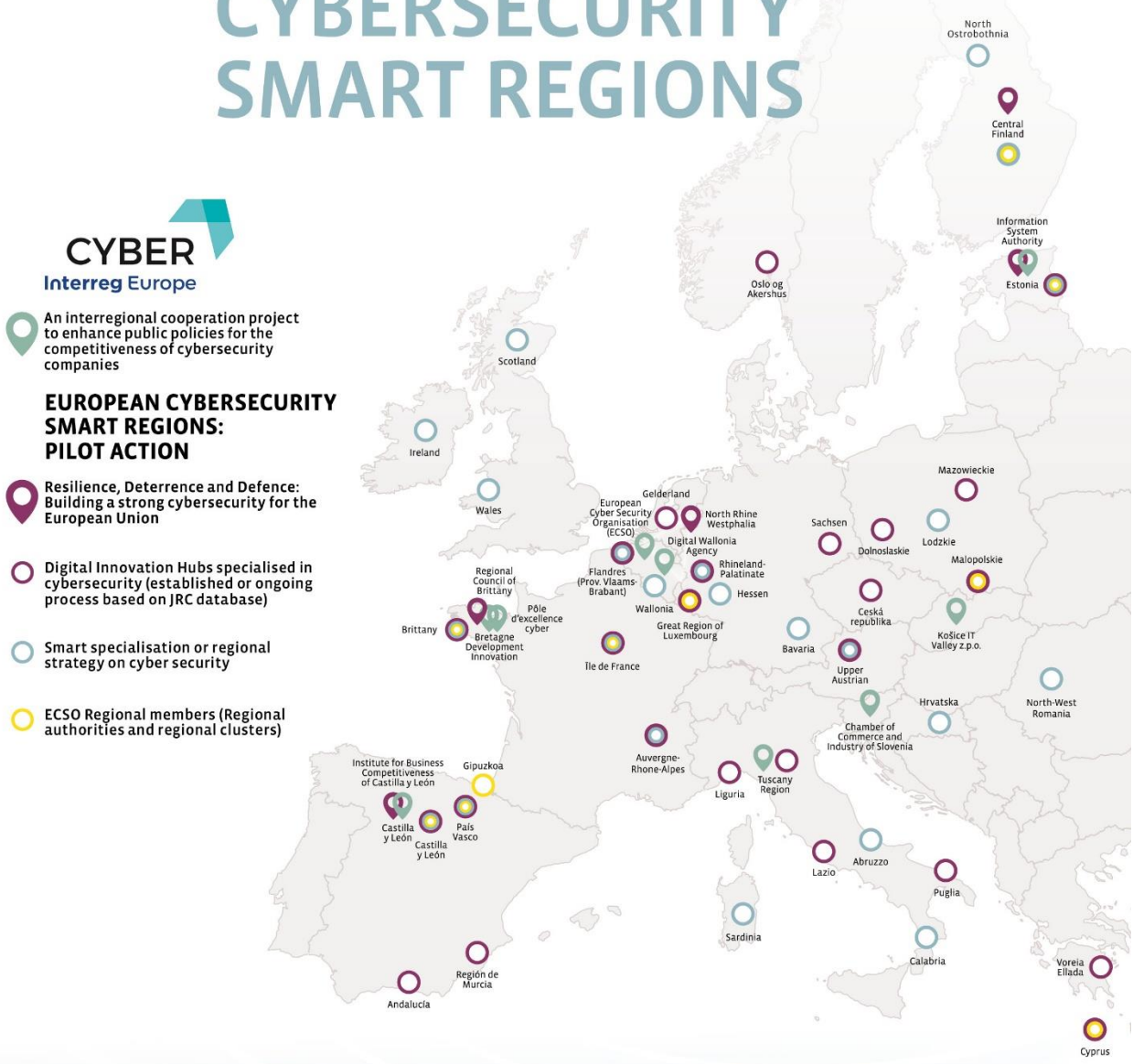
EUROPEAN CYBERSECURITY SMART REGIONS: PILOT ACTION

Resilience, Deterrence and Defence: Building a strong cybersecurity for the European Union

Digital Innovation Hubs specialised in cybersecurity (established or ongoing process based on JRC database)

Smart specialisation or regional strategy on cyber security

ECSO Regional members (Regional authorities and regional clusters)



ECS EUROPEAN CYBER SECURITY ORGANISATION · Région Bretagne · BRETAGNE DÉVELOPPEMENT INNOVATION · European Union European Regional Development Fund · PÔLE D'EXCELLENCE CYBER

1. Introduction

At a time of an evolving landscape of threat, Member States' have an increasing fundamental role in shaping the cyber security industrial landscape as well as national public administrations have a central role to preserve sovereignty issues. While investigating the European cyber security ecosystem, other essential players emerge along national authorities: the regional ones. Uniquely positioned, they hold a privileged connection to their local ecosystems.

Global awareness of cyber security and competitive innovation are reached thanks to a structured cooperation of the regional authorities with their local end-users, critical industries and services, competitive and innovative SMEs, cutting edge R&D labs and training centres.

In the near future, the European Union cyber security landscape will be shaped by initiatives having a direct impact on regional ecosystems, such as the European Cybersecurity Competence Centre and Network, the European digital innovation hubs and renewed smart specialization strategy in each region.

Considering these objectives and the challenges to reach them, the ECSO position paper aims to shed a light on the significant role of regional ecosystems in the post-2020 European cyber security landscape.

2. Why do "smart territories" and regional-level practices matter?

2.1 Critical challenges to the European cyber security market

Europe is both a beehive of cyber security activities and a greenfield of opportunities for traditional and emerging providers. With a domestic market valued at EUR 25 billion and a very diverse industry landscape, made of 12 000 companies of which 74 % are micro companies and SMEs (source: 2018 ECSO Estimation), the European offering is not yet consolidated due to:

- Difficult access to the market for young companies specialised in cyber security
- Strong fragmentation across the different market segments
- Solid divergences among national approach to the market itself
- Lack of critical amount of private investments

However, Europe can count on several 'hot spots' where Research & Innovation and training institutes, as well as end-users and public administrations work closely together. In the future, these hot spots are also expected to become in the future Digital Innovation Hubs – DIHs. Although the European Union has a well-recognized industrial landscape for cyber security, the size and capacity remain less significant compared to its global competitors. In addition, the EU remains a global net importer of cyber security products and solutions and largely depends on non-European providers. This poses a major challenge considering the current risk of disruption of trust due to the large usage of foreign technologies and presence of foreign companies held by third-part countries.

In this context, the 2017 EU Joint Communication "Resilience, Deterrence and Defence: Building a strong cyber security for the EU" underlined that cyber security requires a comprehensive cross-policy approach involving the whole economy and all levels of government, including local and regional authorities.

Similarly, ECSO advocates a multiscale approach to the European industrial policy and a fruitful collaboration between the regional, national and European layer. More specifically, ECSO considers the inter-regional cooperation as a game changer in overcoming the aforementioned challenges. A strategic regional alliance of mature cyber security ecosystems can effectively address issues which are not solvable at a centralised level.

2.2 Successful regional frameworks and mechanisms for innovative and competitive cyber security ecosystems

The regional approach to cyber security goes beyond a simple administrative intermediary role. It is a fully-fledge layer in enhancing cyber security and creating trust. Regional activities play a fundamental role in structuring the sill "young" European cyber security landscape.

ECSO received 11 contributions from European regions with a specific interest in cyber security. The added-value of regional engagement in cyber security is highlighted through key examples of existing regional initiatives and related policy and financial tools.

STRATEGIC PLANNING & DECISION MAKING

Regions elaborate their own economic and innovation strategy - known as Smart Specialisation Strategy (S3).

Regions have the privilege of operating close to local businesses, academia, education and training players. Innovation, economic growth and social development, all happen at the local level. S3 approach invites regions to identify their key sectors for generating investment and the required actions to reach excellence and development. Thus, the S3 aims to increase synergies between different European, national and regional policies, as well as public and private investments. To maximize its global impact, the EU needs more regions having a more solid knowledge of their own specialization. In 2017 the Joint Research Centre counted 18 Regions prioritizing cyber security in their S3. Today ECSO has mapped 25 sustainable local strategies (e.g. **Brittany**, **Central Finland** and **North Rhine Westphalia**) addressing the emerging challenges posed by cyber security and the increasing digitalisation of the society.

In addition to focusing on specific sectors, the regional strategy shall also be coherent with national and European ones. An alignment among these strategies will guarantee the best results. In this regional-national-European approach, the governance model will be the backbone of the desired coherence between the different layers of authorities.

By structuring local ecosystems, regions are the key players in bringing together the European institutions, the R&I stakeholders, **local industry and national operators and administrations.**

A recent move has been detected over the last two years: 31 Regions[1] (e.g. **Castilla y Leon**, **Luxembourg**, **Basque Country, Paris Region, Brittany Region**) have established or are in the process to establish **Digital Innovation Hubs** providing tailored services on cyber security domain. For instance, **Business Upper Austria** will be one of the 11 Digital Centres on the Austria "Cyber Security" Digital Innovation Hub".

Successful smart specialisation strategies (RIS3) and recent DIHs endorsed by regions, as mentioned in the Annex Success story**,** prove the significance of including them as a major layer for the development of European policies.

LONG-TERM INVESTOR & SUPPORTER OF THE "MADE IN EUROPE"

Regions are the managing authority for the European Structural and Investment Funds (ESIF).

In addition to regional funds, the ESIF are considered as a structural tool to support regions in becoming attractive place for companies, research and training organisation specialised in cyber security. Some regions have used the European Regional Development Fund (ERDF) in support of their S3 as crucial resource to enhance cooperation, innovation, and support to SMEs providing cyber security solutions. The ERDF also helps facilitate experimentation, develop R&I project and finance education and training. However, ECSO notices among the received contributions from Regions, that a majority is not aware of the opportunity of using the ERDF to support cyber security projects. Besides, regions themselves support the growth of their local SMEs by facilitating the link with potential end-users or accessing to investors.

A region can encourage convergence and complementarity between projects supported by both the European Strategy Forum on Research Infrastructures (EFSRI) and Horizon 2020 in its territory. For instance, the development of excellence in major research infrastructures is supported in synergy by the ESIF, regional credits and Horizon 2020.

> Through the Structural Funds, **Brittany (France)** finances the competitiveness of Breton players in the European area. For this, the region provides support services in submitting H2020 projects (more than 150 projects tagged S3 actors have been funded since its launch in 2014). The ERDF Funds have been used in the establishment of a federating programme at regional level for research, training and innovation. In addition to national funds, this has been based on

[1] See the map "Connecting European Cybersecurity Smart Regions", page 2. The Joint Research Centre (JRC) databases (e.g. Eye@RIS3 and Digital Innovation Hubs catalogue) are the main sources on the related-data to DIHs and S3. The keywords used for the research on the data base are: "cybersecurity", "cyber security", "cyber-security".

platforms for experimentation and use testing (e.g. technical support to platforms, development of cyber security chairs in partnership with industry, training courses, call for ICT and defence projects).

In **North Rhine-Westphalia (Germany),** a regional open call to provide public funding for SMEs was backed up by the ERDF (*Leitmarktwettbewerb IKT.NRW*). It has been successfully used to integrate SME into complex projects (e.g. critical infrastructure protection, artificial intelligence).

With support of the funding from the Regional Council of Central Finland, a cyber security certification scheme was developed for SMEs, the FINCSC – Finnish Cyber Security Certificate). In **Central Finland,** the "Kasvu Open" competition operates every year, which is the largest programme for sparring eager to grow companies (especially SMEs) with growth experts in Finland. Kasvu Open programme received the European Enterprise Promotion Award from the European Commission in 2018.

The **Paris Region (France)** brings together cyber security actors in a "Cyber security Forum" and allocated €1 million to an innovative challenge for cyber security SMEs. While the ERDF projects are multiannual and coordinated by the regional cluster Systematic Paris Region, the Paris Region has also set up mechanisms to support the growth of SMEs. Among these grants, Innov'up allows SMEs to set up R&D activities by supporting them up to €100k in the form of a grant and €1M in repayable advance. PM'up supports projects to develop the company's activities up to €250k.

THE TRIPLE HELIX SYSTEM: *From Innovation to commercialisation of competitive solutions*

Regions host a triple helix system offering a truthful environment for innovation to the market.

Thanks to a great proximity to local players, regional administrations players are driving force in the development of local innovative and competitive ecosystem. As such, they are a core part of the triple helix, also known as the "golden triangle" involving governments, academia, and businesses. Regions participate to sustain the cyber security value chain in the EU Member States - by involving RTOs, training centres, services operators, incubators, SMEs and established large companies.

In **North Rhine-Westphalia (Germany)**, universities, local and regional authorities, business associations as well as established companies support start-ups by providing advice on business models and technology readiness. More than 20 cyber security startups (mostly spin-offs from local University and Research Centres) are free to attend

industrial and career fairs. Teams are formed interdisciplinary and professors are regular members of the management boards. Business plan competitions, pitches and networking events complete the regional offer.

Regions are familiar with local businesses fabric and develop tailored SME funding scheme dedicated to them.

Wallonia Region (Belgium) initiated a new regional mechanism for cyber security awareness among SMEs - "Keep IT Secure" which targets SMEs through a controlled network of cyber security providers. Currently the Region has taken an active role in setting up an operational cyber security scheme for raising the maturity of SMEs. It is based on a cluster of security experts. IT Research centres like CETIC are supporting its operation.

Regions are the main intermediary for the successful implementation of national programmes for innovation.

In Spain, a supportive program for "Public Procurement of Innovation" was introduced on the national level under the general "Public Services Procurement Law" and applicable at a regional, provincial, and local level. As such, the *Instituto para la Competitividad Empresarial* (ICE) in **Castilla y León (Spain)**, among various programmes, has developed an innovative support scheme to SMEs to encourage, from the demand side, the innovation and technological development of local companies specialized in cyber security. In particular, the ICE has development a work plan that includes the development of a Pre-Commercial Public Procurement programme which allows the acquisition of solution based on R+D+I.

Lastly, Regions demonstrate the capacity to lead the development of key platforms to support investment in SMEs (both providers and end users) through the Triple Helix:

In **Basque Country (Spain)**, the Regional Government and local councils have developed regional tools to foster entrepreneurship and business development. Acknowledged by The Financial Times Strategy Awards among 171 Agencies world-wide in different categories, the Basque Country received the First-Prize winner in "Start-ups and SME support" category thanks to the Acceleration Program Bind 4.0. This startup accelerator programme gives investors access to the Industry 4.0 customers. Also, it received the Second-prize winner in "Incentives" category" with the "Invest in the Basque Country' services" incentive, bringing together Research, Development and Innovation while stimulating investment in local startups and SMEs.

In the **Great Region of Luxembourg** there is a huge support from the Ministry of the Economy, via its agencies, SECURITYMADEIN.LU and Luxinnovation. A success example is the cooperation in the context of the Fit4Digital accelerator programme for SMEs. SECURITYMADEIN.LU developed "the CASES Diagnostic" to help SMes identify IT risk exposure. Thanks to Fit4Digital programme, this service is promoted and deployed via Luxinnovation'.

Cyber Wales (United Kingdom), as a network of businesses, academia, law enforcement and Defence, and Government has been highly effective in ensuring that security messaging is consistent and follows the lead of the National Cyber Security Centre, across Wales. There are several SME growth initiatives within Wales that are accessible to cyber related to businesses. These are provided directly by agencies such Welsh Government, Local Authorities and the Development Bank of Wales and indirectly through partner organisations. Programmes such as the Accelerated Growth Programme seek to support the growth and scale up of high potential small and micro businesses and have helped many businesses.

Castilla y León (Spain) contributes to an international acceleration program involving three entities in the region (INCIBE – Spanish National Cyber security Institute, City Council of León and Institute for Business Competitiveness of Castilla y León). The program consists on the promotion of entrepreneurship in Cyber security by supporting the talent attraction, the generation of business ideas through their incubation and the acceleration of entrepreneurial projects.

All the triple helix actors are located at the regional level. Thanks to regional or national means, these organisations support the emergence, development and implementation of innovation.

Brittany (France) relies on the strengths of the Ministry of Army with the DGA-MI (i.e. Centre of expertise in cyber security) which has a world-class civil training and research ecosystem with more than 200 researchers working exclusively on identified cyber issues and 2800 trained students per year. Set up in 2014 under the aegis of the French Ministry for Armed Forces and the Regional Council of Bretagne, the "Pôle d'Excellence Cyber" As a non-profit-making association, this leading organisation brings together civilian and military, public and private, academic and industry key players.

PROXIMITY WITH END-USERS & CRITICAL INFRASTRUCTURES

Regions are accessible territories of experimentation and connection with end-users.

The proximity with end-users (i.e. operators and citizens) makes the regional level considerable in disseminating good practices as well as in establishing

preventive measures and immediate response services. Regional level is a mandatory step in reaching a global European awareness in cyber security. Also, regional authorities are direct users of cyber security solutions when developing their services (e-gov, smart cities, health, etc). It goes without saying that as potential of victims of cyber-attacks, Regional authorities share valuable information with local infrastructures.

> **Britany Region (France)** has invested in the development of cyber security for 2014-2020. As a flagship initiative, Brittany has launched a joint initiative with the French Ministry of Defence, INRIA and Centrale Supelec to develop the Joint High Security Laboratory in Rennes. This research infrastructure aims at facilitating R&T transfer in cyber security in the region. In particular, the centre hosts a platform to test informatic virus and security evaluation which are also open to the industry. Another example shows that the Chair of Cyber Defence of Naval Systems (i.g. developed by the ITM Atlantic, Naval Group, Thales, ENSTA and the Naval School) covers the naval component of cyber defence with the support of the Brittany Region and the Cyber Centre of Excellence.

Regions are also a layer for experimen**tation for vertical platforms and testing of solutions for local end-users**.

> **Basque Industry 4.0 initiative (Spain)** promotes Industrial Cyber security, especially projects that address the convergence and integration of protection systems against cyber-attacks for IT/OT (Information Technology / Operational Technology) environments in industrial manufacturing companies. The project subsidies for Industrial Research and Experimental Development projects that involve technology transfer from technology providers to industrial companies, in the field of EICTs applied to Advanced Manufacturing.

REDUCING CYBER SECURITY SKILLS SHORTAGE

By supervising education and training, regional authorities play a key role in addressing cyber security skills shortage.

As well known, the is an urging need of IT specialists and in particular of cyber security experts for both business and research tasks[2]. In addition, because of the lack of harmonised carrier paths and clear professional opportunities at European level, Europe experiences also an outflow of highly qualified specialists to other markets. In this context, the pipeline of experts and talents coming from regional endeavours organising the training and education in their territory is fundamental considering the raising needs of operators and cyber security providers across Europe.

[2] According to the *2017 Global Information Security Workforce Study*, Europe faces shortage of 350,000 cyber security professionals by 2022

The government of **Upper Austria** supports in the University of Applied Sciences at Hagenberg – Secure Information Systems Department – to provide SMEs with highly skilled specialists in cyber security. Currently, at least three companies with employees from the University are providing expertise, services, solutions, and consulting in cyber security.

Since 2011, **Central Finland** has initiated a series of projects co-financed by ERDF aiming at the specialization on the training of cyber security skills. In particular the JYVSECTEC (Jyväskylä Security Technology) is a successful simulation environment for cyber security management systems as well as a development platform for competence building. Recently the JYVSECTEC project has launched a specific platform to support the national healthcare (Health Care Cyber Range 2019-2021).

3. ECSO as a laboratory of innovative ideas and exchange and implementation of the best practices with regions

Since the signature of the Public-Private Partnership on cyber security (cPPP) with the European Commission in 2016, ECSO dedicated a specific Working Group designed as a laboratory of exchange and ideas on interregional cooperation. From that moment onwards, the regional community of is growing within ECSO. In 2018, this endeavour led to an official participation from ECSO and some regional members to two European interregional projects in cyber security.

1) **ECSO engaged as Advisory and Communication partner to INTERREG Europe CYBER,** for which the European Regional Development Fund has invested EUR 1.53 million. This 5-year project is led by Bretagne Development Innovation and involve the public authorities from 7 EU Regions. Together, regions will exchange best practices on improved public policies to support local SMEs and create synergies among the European cyber security ecosystems. The main goal is understanding and sharing public policies that can help knock down barriers of market fragmentation, lack of coordination of regional actors and lack of skills.

2) **ECSO supports as "Single Partner Coordinator" the European Commission's Pilot Action on Smart Specialization in cyber security**, which involves Brittany (Leader), Estonia, North Rhine Westphalia, Central Finland, Castilla y Leon. This interregional partnership "European Cybersecurity Smart Regions" project aims to develop interregional cooperation, boost the commercialization and scaling-up phase of local competitive companies, foster business investment on cyber security. In 2019, the priorities of the Pilot Action will focus on:

- Finalizing and deploying the mapping of the 5 regional ecosystems thanks to a joint tool that visualizes capabilities (e.g. Identify, Protect, Detect, Respond, Recover) and the type of local actors (e.g. companies, research centres, training labs, support structures). Based on a legal agreement, data are shared by different regions.

- Designing an interregional acceleration programme to create a market place with reduced costs for local SMEs to commercialise their solutions.

4. Post-2020 cyber security landscape for regions

Smart Specialisation in cyber security and inter-regional cooperation should become a permanent feature of the post2020 European cyber security ecosystem. This would ensure a multiscale cooperation in reducing market fragmentation and supporting the European industry competitiveness. When defining the EU "position to autonomously secure its digital assets and to compete on global cyber security market", a set of recommendation is listed below to place the regions at the heart of the EU strategy.

1) The foreseen European Cyber security Centre (ECC) and Network of National Coordination Centres (NNCC) should build on the experience of ECSO and guarantee a role to Regional authorities in the future governance.

As argued, the European regions play an important role in contributing to the economic growth thanks to leverage effect of regional means. Regions aim to play a key role in establishing traction between European-level institutions and programmes on the one hand, and local ecosystems on the other hand. For instance, the SPARTA pilot Cyber security Competence Network brings together 14 EU Member States with 44 actors. In this Pilot, regional clusters such as Systematic-Paris-Region and the Pôle d'Excellence Cyber are involved as Associate Partners.

In this context, ECSO advocates for a multiscale approach by attributing to regional authorities a place in the governance of the future European cyber security. The role given (i.e. definition, decision, management) shall be enhanced although conducted in close collaboration with the European Commission and national authorities. Such action would contribute to avoid overlap, create ties between national and regional bodies (e.g. smart cities and DIHs), and bring the priorities identified by the ECC and NNCC to the local level by a bottom-up approach. Finally, strengthening cooperation across European regions shall remain fundamental in the new framework.

ECSO already does this within its Working Group dedicated to support SMEs and regional cooperation.

2) Forget the "Silicon Valley", an inter-regional network of smart territories would accelerate the commercialisation of solutions "Made in Europe"

No one shall have as objective to replicate existing mature ecosystems (e.g. Silicon Valley in the US or Beersheva in Israel). It is obvious that every global ecosystem will continue mutual analyse and learn from one another. However, ECSO strongly believes in recognizing and taking advantage of our own European distinctive strengths and values.

The EU should play as a geographic constellation of "Cybersecurity Smart Regions". In this scenario, each regional ecosystem contributes to a common programme and facilitate a quick access of local cyber security SMEs to the European market. This would impulse a still-missing critical mass of growth companies to stay at the leading edge and build high-growth European companies globally competitive. Finally, this would be the best to attract much more private investors.

The ongoing Pilot Action aims to fill the commercial expertise gap. It will bring to local scaleups an expertise from a network of "Cybersecurity Smart Regions" and private investment to co-found. The SP3 action represents a good start in getting local scaleups on the European map, but much more remains to be done to reach out more Regional ecosystems.

Regions play a key role for economic development and innovation support. Considering this major element, the two following actions shall be considered by the European Union to improve the impact of the invested funds:

- Enlarging existing European financial framework such as the ERA-NET programme for a regional usage in the field of cyber security to support collaborative R&D projects;

- Defining a common financial mechanism to support the development of dual-use innovations at EU level, whose programme would specifically address end-users.

3) Regional authorities as efficient managing authorities of European funds

The territorial dimension of the Horizon Europe programme shall be developed in order to improve its impact at regional level. Regions can also be levels of experimentation at local level. The Horizon Europe programme shall better integrate into the calls the structures representing, for instance, the regional research and innovation ecosystems (e.g. poles of excellence, competitiveness or clusters).

Some Regions have expressed the important need for Regional intermediaries to manage decentralized financing, namely "cascading funds" as it has proven to be a very efficient mechanism for supporting companies in the adoption of new technologies. Adoption of cascading funding mechanisms in Horizon Europe calls on cyber security is recommended. Increasing such mechanism shall also be considered in the deployment of technologies or testing and experimentation with end-users (particularly for areas related to S3).

4) Enabling synergies between European Structural and Investment Funds and Horizon Europe and beyond as part of European competitiveness strategy

Regions should develop synergies with other existing initiatives to improve the leverage effect of current regional actions. Although Horizon Europe and ERDF (under the Cohesion policy) have different objectives, the first focusing on excellent in R&I while the second on incremental research and uptake of already existing innovation, Regions can play the role of bridge builders between the two funds.Regions can choose to locally encourage convergence and complementarity between the projects supported by the EFSRI and Horizon Europe. For instance, the ESIF, regional funds and Horizon Europe can jointly support the development of major research infrastructures. Therefore, a better articulation between Horizon Europe and operational programmes would maximise the impact of European funds and facilitate synergises among existing initiatives.

In the context of the Regions' Smart Specialisation Strategies (RIS3), more European projects should be encouraged in the next Horizon Europe programme. Relations between the European institutions and the Regions will have to be strengthened in order to meet the challenges of FP9, particularly in terms of readability, renewal of beneficiaries, adequate prioritisation and simplification.

5. Regions play a catalyst role in Europe's cyber security

European Regions are the "laboratory for innovation and change" (Lamy report).

Encouraging mature regional ecosystem will accelerate the cooperation among them. Such dynamic will benefit regions themselves by improving the visibility of their successful, sustainable and innovative ecosystem. As stated by regions, a multi-layered approach involving cyber security regional ecosystems do create business opportunities, such as identification of new partners or expansion of local cyber security companies and attract talents and investors.

Diversity in organisational set-up, vertical specialization and financial supporting characterizing the European territories is not an obstacle to create a true European model of cooperation. It is rather, a unique opportunity for consolidating a European cyber security model and ecosystem.

It is surely time to move forward and understand that the European Cybersecurity Smart Regions have a great value to support the competitiveness of the industry and innovation. Involving regional capacities in the future EU cyber security strategy will create the necessary bridge with the common objective to become a global leader in this field.

APPENDIX - "Smart territories" in cyber security: Success stories

1. Basque Country, Spain (Inhabitant: 2.2 Million)

Local Cyber Security Companies: A total of 107 organizations provide Cybersecurity services or technologies in the Basque Country:

- Distribution:
  - 82 private companies (69 of them were born and have their TaxID located in the Basque Country), employing a total of 1.749 people in Cyber Security.
  - 3 Public Institutions
  - 4 Universities
  - 7 RTOs
  - 4 Vocational Training Centres
  - 7 non-profit Associations.

Success Story: Our Cyber ecosystem began in 1991 when Panda Security was born in Bilbao, the first Spanish cyber security company with nearly 500 employees at present. The biggest, the oldest and the most internationalized Spanish Cyber Security pure players (Panda Security, S21sec, Innotec System) are Basque Companies. One third of the Spanish Cyber startups are concentrated in the Basque Country (21 at the end of 2018).

The special conditions of the capacities offered by the region to promote Research, Development and Innovation for high-value technology activities make it possible that every year new Cybersecurity startups emerge in the Basque Country. That's why nowadays a total of 16 Basque Companies produce their own European cybersecurity technology which is designed and developed in the Basque Country, a very remarkable aspect taking into consideration the European dependency on technology from other markets. In 2018 we were reported of 154 researchers working full time on Cybersecurity in the Universities and RTOs of the Basque Country.

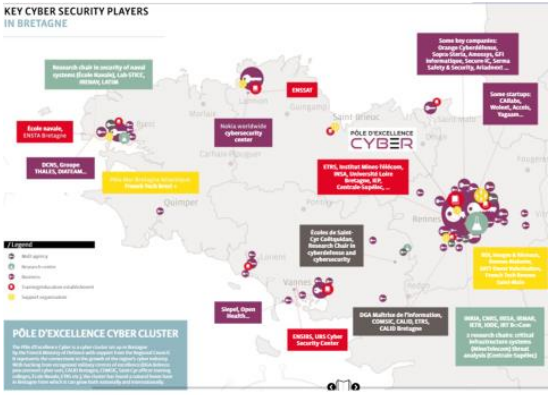
The Regional Government is strongly committed to support SMEs through a variety of instruments including grants programmes, public venture capital, entrepreneurship incentives, and a long etcetera. One of the most internationally acclaimed and acknowledged initiatives is the BIND 4.0 programme (www.bind40.com) that provides a platform for technological SMEs to answer the challenges posed by 42 big industrial companies established in the Basque Country and working for RIS3 sectors. The last edition of this programme included 6 cybersecurity startups out of 32 selected startups. BIND 4.0 has been recently awarded with the first-prize by the Financial Times Strategy Awards 2018 in the category of "SME Support", the Basque Country has also been recognised in another 3 categories.

Web Site: https://www.basquecybersecurity.eus/en/

2. Brittany, France (Inhabitants: 3.329 million)

Local Cyber Security Companies: According to the analysis carried out at regional level, around 130 businesses work in cybersecurity in Brittany, including more than 100 SMEs delivering technological solutions covering the whole cybersecurity value chain.

Success Story: A 2014-2020 program for the development of a cybersecurity ecosystem of excellence in Brittany Region.



Brittany Region has defined cybersecurity as a priority of its Regional Strategy for Smart Specialisation (RIS3) for the 2014 – 2020 period. This was based on its regional strength, which includes strong ICT and defense sectors. The Regional ambition is to become a unique and attractive place for companies, research and training in the cybersecurity sector.

To strengthen the regional cybersecurity industry and support competitiveness and growth of SMEs, the Brittany Region has invested more than 30 million € so far in the development of cybersecurity for the 2014-2020:

- A Partnership Agreement Signed for Research And R&D Development between DGA, Brittany Region and RTOs and university (e.g. CNRS, INRIA and 11 academics) for a doctoral and post-doctoral grant: 12 M€ over 6 years.
- High security laboratory in Rennes: a joint Initiative with DGA, Brittany Region, Centrale/Supelec school and research institutes INRIA and CNRS. Strong links with the industry focus on treat analysis purposes. It facilitates research and technology transfer in cybersecurity in the region, including large companies and SMEs (e.g. Secure IC).
- Creation of a regional distributed infrastructure with 6.3 M€ investment program in platforms to develop a network of competences in reseach, education, and innovation. It is based on National, regional and ERDF funds and will be distrusted all over our territory.
- 4 Industrial chairs with big companies and SMEs including naval systems, critical infrastructure, threat analysis, cyber defence and crisis management.
- Innovation & economic development: launch of several call for projects Brittany Regional Council organizes calls for cyber security projects worth a total of 1 M€.

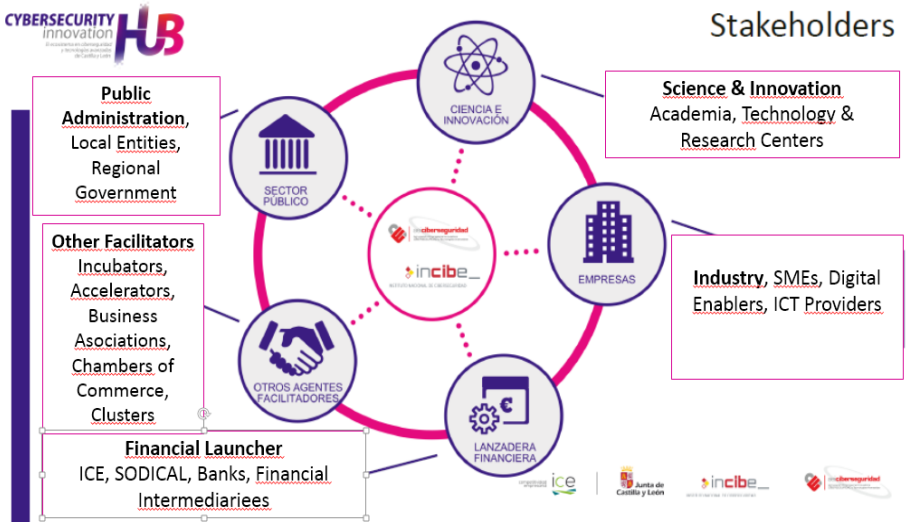
Website: https://www.bretagne.bzh/

3. Castilla y León, Spain (Inhabitants: 2.4 million)

Success Story: Cyber Security Innovation Hub.

The **Cybersecurity Innovation Hub** is a digital ecosystem around cybersecurity and advanced technologies to bring the benefits of digitalization to companies and help them accelerate their adoption of digital technologies. INCIBE, the Spanish National Cybersecurity Institute, as a reference center, the Institute for Business Competitiveness of the Regional Government of Castilla y León (ICE) and the Association of Innovative Companies in Cybersecurity and Advanced Technologies have established together.

The Cybersecurity Innovation Hub is organised around an existing ecosystem. The activities and services are used around a unique strategy. The transfer to the industrial sectors is the main objective as well as to improve companies' knowledge of security policies and support them in their digital transformation processes.



Main activities and services of the Cybersecurity Innovation Hub include:

- Demo spaces giving user companies access to infrastructure to test the adaptation of different technologies.
- Co-development through company-client activities from which projects may arise with or without public funding.
- R&D by including mapping of R&D competencies and implementation of collaborative projects.
- Recruitment of professionals through the promotion of programs stimulating talent, recruitment and return of professional to counter the lack of experts.
- Entrepreneurship promoted through incubators and business accelerator.
- Specialized training addressed to technological and industrial sectors in advanced technologies and cybersecurity.

4. Central Finland, Finland

Success story: JYVSECTEC – Finland's leading Cyber Security research, development, and training center

JAMK University of Applied Sciences based JYVSECTEC is a cyber security exercises and trainings provider. The exercises and trainings developed and created by JYVSECTEC are a holistic way to improve organizations' capabilities and knowledge to defend against cyber threats.

JYVSECTEC was created in 2011 and was developed using three major R&D projects: JYVSECTEC, JYVSECTEC CENTER and JYVSECTEC CENTER RGCE which all have enabled us to build our expertise and one of the most advanced cyber range in the world. Main financiers of R&D projects were Regional Council of Central Finland and European Regional Development Fund (ERDF).

As a part of the development, the state-of-the-art cyber range Realistic Global Cyber Environment (RGCE), along with the thorough expertise of JYVSECTEC, has been recognized in Finland and international markets as well. With the RGCE cyber range, the JAMK UAS achieved the status of cyber security experts, and signed co-operation agreement with the Finnish Ministry of Defence on the development of national cyber security in 2013. JYVSECTEC has organized Finland's national cyber exercises annually since 2013. The RGCE cyber range has achieved the status of the Finland's national cyber range.

Alongside with the national cyber security exercises, JYVSECTEC is a known partner for helping critical infrastructure organizations and companies to enhance readiness and resilience against modern digital threats. In addition, JYVSECTEC has launched the Finnish Cyber Security Certificates FINCSC and FINCSC PLUS.

JYVSECTEC is an active member of the European Cyber Security Organization (ECSO), European Defence Agency (EDA) projects and European Defence Fund projects. Since 2014 JAMK has been involved as coordinator or partner in Horizon 2020 proposals and works as partner in one of the four European Cyber Security Competence Network projects called CyberSec4Europe starting in February 2019. Recently JYVSECTEC has commenced a project Healthcare Cyber Range, which develops Cyber Security training and exercises for healthcare organizations, through implementation of healthcare services, as part of RGCE Cyber Range. JYVSECTEC is solidly dedicated to becoming a globally trusted partner in forthcoming R&D activities, both in cyber security and other ICT related issues.

Website: https://jyvsectec.fi/

5. Luxembourg and the Greater Region (Inhabitants: 11.6 million inhabitants from 5 regions, 4 countries speaking 3 languages)

Local cyber security companies: Close to 200 companies are active in the area of Cybersecurity in Luxembourg and the Greater Region. A detailed market analysis is the making and will be published in fall 2019.

Success Story: The SECURITYMADEIN.LU ecosystem:

SECURITYMADEIN.LU is the main source for cybersecurity in Luxembourg. Created in 2010, it builds on the integration of the pre-existing services, infrastructures, platforms, experiences and competences of partners, and thus represents a central place for information security awareness-raising, news, tools, support and problem-solving material. On its online portal, all news, events, tools and other valuable information from the Luxembourg Cybersecurity Ecosystem are centralised.

Following, the impulse of the Ministry of Economy in Luxembourg, SECURITYMADEIN.LU's focus is threefold:

1. Accompany SME's via projects like Diagnostic CASES, Fit4Digital, Awareness sessions, Incident Response. In close collaboration with the Chamber of Crafts a "cybersecurity follow-up programme" (e.g. similar to the one in Wallonia) is being beta-tested
2. Foster and partner with local entities to share expertise and co-innovate, addressing market gaps (e.g. monthly cybersecurity breakfast & newsletter ; Cybersecurity Week Luxembourg; eBRC, partner of ROOM#42 (the cyber-attack simulator))
    - A security testing services for start-ups is in the making
    - Deployment of MONARC via our partnership with the CCB in Belgium
3. Outreach, collaboration and cooperation within the Greater Region and beyond: Encryption Europe Alliance (involving companies from FR, DE and LU); European gathering at ICTspring; partnership building with CISPA (DE), Galaxia (BE) and CNAM (FR); partner of the "Greater Region Forum" and "Get2Know initiatives"; common presence at international fairs like FIC in Lille

Website: https://securitymadein.lu/

6. Bochum and the Metropolis Ruhr, North Rhine-Westphalia, Germany (Inhabitants: 5.1 million)

Local cyber security companies: 53 IT-S companies, 20 start-ups in the last years, among them: G Data, Materna, Escrypt, secunet Security Networks AG, VMRay, physec, rhode&Schwarz, XignSys, RipsTech.

Success Story: Bochum - a thriving hot-spot for cyber security. Bochum, at the heart of the Metropolis Ruhr is the nucleus of Germany's largest and most innovative cyber security hot-spots. In the regions, the first antivirus program was invented, world-class research is conducted, and innovative IT security enterprises are headquartered. Bochum will be the site of the first Max Planck Institute for Cryptography and Protection of Privacy.

Over 200 scientists, 1200 students and 26 chairs in seven disciplines: Horst Görtz Institute for IT Security (HGI), an institute of Ruhr University Bochum (RUB), is the largest university institute in this discipline in Europe. The HGI is dedicated to research and teaching in virtually all aspects of modern cryptography and IT security.

Bochum University of Applied Sciences, Technische Hochschule Georg Agricola, the International School of IT Security (isits), the Institute for Internet Security (if(is)), an institute of Westphalian University of Applied Sciences Gelsenkirchen, the Paluno institute of the Universität Duisburg-Essen ensure not only a steady stream of young experts but excellent research. **All companies, stakeholders and institutions launched eurobits as an umbrella brand, which brings together leading research institutes, committed companies and young growth enterprises**. The objectives are to coordinate research, initiate educational programmes and facilitate knowledge transfer to the business sector. In 2018, the industry trade show IT Trends Sicherheit posted another exhibitor and visitor record. New event formats such as the hacker conference RuhrSec (hackmanit GmbH) and the JavaScript conference RuhrJS (9elements GmbH) have been successfully launched in Bochum.

Website: https://www.eurobits.de/en/

7. Paris Region, France (Inhabitants: 12.2 million)

Success story: "the Paris Region Cybersecurity Challenge"

The Paris Region made the industry its priority by developing an ambitious Smart Industry strategy with the allocation of €300 million by 2021.

The Paris regional strategy is based on 3 essential axes:

- Projecting companies towards the Industry of the Future and training them with essential needs
- Modernising industrial activities, such as fabrication
- Boosting the image of Ile-de-France industry

Cybersecurity is considered as a major economical challenge for companies and has been defined as a technological priority for the Paris Region, which is a leader in cybersecurity in France with 80% of the jobs in the sector, 60% of companies offering solutions, and 25% of the higher education offer.

> In November 2018, the "Cyber security Forum" was hold in Paris. This regional conference on cybersecurity is part of a global approach undertaken by the Paris Region with cybersecurity partners, including the research and private sector. As leader in advanced technologies and industry, the Paris region announced at this occasion an innovation challenge: "the Paris Region Cybersecurity Challenge". The Paris Region has allocated €1 million to this innovative challenge for cyber security SMEs for which the three best start-up projects will receive a financial support to their R&D activities. The challenge is organized in partnership with the Systematic cluster, Hexatrust club, CEA, Deloitte, Atos, SNCF and the Stade de France.

The attractiveness of the regional ecosystem is supported by Systematic Paris-Region. This innovation and technology cluster brings together over 900 members and promotes an ecosystem of excellence in digital technologies. In the Cyber & Security domain, Systematic Paris-Region has a strong core of 224 members, including 120 SMEs, 50 large groups, 50 universities and academic centres, and covers 4 local territories. Its roadmap covers 10 technological areas, including among others Critical Infrastructure, Smart territories, Energy and Utilities, Industry 4.0, Health, Enterprise IT, Public authorities and Defense. Systematic connects stakeholders, boosts innovation through collaborative R&D projects, SMEs competitiveness (e.g. access to finance), and providing an efficient business sourcing.

Website: http://www.systematic-paris-region.org/

8. Wallonia, Belgium (Inhabitants: 3.61 million)

Local cyber security companies: Nearly 15 companies are active in the cyber security field and registered to the regional cluster Infopôle TIC

Success story: KIS - Keep It Secure: a Walloon cyber security mechanism by Digital Wallonia

In 2019, the Walloon governmental agency for digital topics (Agence du Numérique) launched a dedicated cybersecurity mechanism called KIS: for Keep It Secure, which is part of the Digital Wallonia programme.

The region addressed the urging topic of cyber security and the needs of companies. The new mechanism is included in the broader regional subsidies system called "corporate checks" (chêque d'entreprises). It provides companies a regional and financial support to enhance their competitiveness and to ensure their cybersecurity.

The regional approach was based on direct feedbacks from the market and from the main service providers. The identified needs correspond to a level of action targeting the service providers active in cybersecurity and companies and more specifically SMEs.

The main objective is to create a "virtuous circle of trust" in which companies are encouraged to invest in cyber security. As a result, local companies progressively gain in skills and can count on certified experts to guide them whilst being financially helped by the region.

The KIS regional mechanism is based on a framework of specific skills which assess the cybersecurity professionals eligible to perform through the corporate's checks system. For its development, this framework has been based on various examples in the EU such as the UK's Cyber Essentials. Two Walloon research centers developed the framework of skills and ensured its compliance with existing and future initiatives.

Local companies can use this regional mechanism to improve their knowledge and increase their cyber security. In addition, this mechanism is a market differentiator through which companies gain visibility and attract or reassure their customers-clients.

Website: https://www.digitalwallonia.be/fr/publications/keepitsecure

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU