



Multi-level Governance in Cybersecurity: What Role for the European Regions?

MILDA KAKLAUSKAITĖ

POLICY MANAGER, EUROPEAN CYBER SECURITY ORGANISATION (ECSO)

Introduction

In its first ever cybersecurity strategy adopted in 2013, the European Union (EU) stated that it aims to “make the EU’s online environment the safest in the world” (European Commission, 2013). Since then, a number of policy measures have been implemented to strengthen the EU’s cybersecurity capabilities and resilience against cyberattacks, including the Directive on security of network and information systems (NIS Directive), Digital Single Market Strategy, the proposal to create the European Cybersecurity Competence Centre and Network, the EU Cybersecurity Act, as well as the Digital Europe and the Horizon Europe programmes. While cybersecurity’s place at the top of the EU’s political agenda raises no doubts, the question of key actors in charge of strengthening the EU’s cybersecurity requires wider debate at both strategic and operational levels.

The concern regarding the key EU cybersecurity actors is a primary focus on the European and national level. The current EU policy suggests that in the context of cybersecurity the principal players are Member States’ national governments, supported by the dedicated EU bodies, such as the European Union Agency for Cybersecurity (ENISA). The role of European regions is largely omitted. However, the regions are what has the biggest potential to connect the technology with the end users, assist local small and medium enterprises (SMEs), and provide them with business support and access to innovative technologies. In order to achieve an effective cybersecurity posture, the EU must realise that national governments and EU institutions are not enough and that more structured inclusion of the regions and the definition of their strategic role

in Europe's cybersecurity is needed. Therefore, this paper argues that the multi-level governance model needs to be established to include European regions in the EU cybersecurity policy implementation.

The regions are what has the biggest potential to connect the technology with the end users, assist local small and medium enterprises (SMEs), and provide them with business support and access to innovative technologies.

Cybersecurity and the changing roles of the state

The traditional approach to security highlights the state as the main referent object of security and the key actor in implementing security politics. Historically, and especially after the establishment of Westphalian sovereignty, the states have had an exclusive authority within their territory and the right to legitimate exercise of power to ensure its security against any external threats. Such security-sovereignty nexus has become deeply enshrined in international and domestic political discourse, making it difficult to include other actors in the traditionally state-dominated field of security. However, the emergence of cybersecurity as a political and security issue suggests the changing role of the state as the key security actor.

The emergence of cybersecurity as a political and security issue suggests the changing role of the state as the key security actor.

Because of its multifaceted and all-encompassing nature, cybersecurity policy requires a diversification of the actors involved in its implementation. The increasing digitalisation and the resulting security challenges place cybersecurity at the top of the political agendas across the globe. Unlike the previous "hot" security challenges that have dominated the political agendas for years (e.g. a classic example of nuclear proliferation during the Cold War), cybersecurity cuts across different policy areas and affects the daily social, economic and political life

of entire society.¹ This new security environment changes the role of the state, making it not only the sole security guarantor, but also the security partner (Dunn Cavelty & Egloff, 2019, pp. 42–49). For example, critical infrastructure protection requires the state to cooperate with the private sector, and to raise cybersecurity awareness the state needs to directly involve society. Sharing the authority and responsibility of cybersecurity with the new actors becomes a prerequisite.

The ensuring of cybersecurity becomes barely possible without close cooperation with the non-state or semi-state actors, including private sector representatives, different levels of government, and NGOs organisations. The cooperation with the private sector has been recognised as an important step in strengthening the EU's cybersecurity, resulting in the contractual public-private partnership on cybersecurity signed with the European Cyber Security Organisation (ECSO) in 2016 (European Commission, 2016). At the same time, European regions still lack recognition as important cybersecurity actors. However, it is the regions that can ensure the cohesive EU cybersecurity policy by linking the local users, research centres, and suppliers of cybersecurity solutions with the national and the European levels.

The (in)visible role of the regions

The main advantage of the regions is their proximity and their ability to build trust among the local cybersecurity stakeholders. Unlike national governments, which tend to (and actually must) have a bird's-eye view of the country's cybersecurity posture, regions enjoy much closer connection to the local cybersecurity stakeholders: from end users and integrators to research and innovation (R&I) centres, product and service providers. The *Pôle d'excellence cyber* initiative, launched under the auspices of the

¹ There is no doubt that the disruptive potential and the far-reaching impact of the cyberattacks are widely recognised. However, in the political discourse cybersecurity is not associated with the "doomsday" and all-out war scenarios which are often considered for "hot" security issues and give the state an exclusive authority to act. As a current security policy priority, cybersecurity is more a matter of the "normal", everyday politics and policy practices rather than the politics of emergency.

French Ministry of Armed Forces and the Brittany Region, is a good example of how the state can benefit and advance its cyber readiness by involving the regional authorities in cybersecurity (Pôle d'excellence cyber, n.d.). This privileged position allows regions to effectively address the cybersecurity innovation and industry development issues which could be difficult to manage by national authorities due to their lack of knowledge about regional cybersecurity environment and its dynamics.

The Pôle d'excellence cyber initiative, launched under the auspices of the French Ministry of Armed Forces and the Brittany Region, is a good example of how the state can benefit and advance its cyber readiness by involving the regional authorities in cybersecurity

The regions could play an important role in strengthening national and European cybersecurity posture. In recent years, European regions have become a frequent target for cyberattacks. The ransomware attacks against a Rouen hospital in France (BBC, 2019) and the city of Frankfurt in Germany (Cimpanu, 2019) that happened at the end of 2019 are just a few examples among many others. The regional preparedness against cyberattacks can serve as a litmus test to identify national strengths and weaknesses. Being in a direct contact with the end users, CISOs (Chief Information Security Officers), critical infrastructure operators, and national governments, regional authorities can establish effective response mechanisms and preventive measures, thus contributing to the increased cybersecurity awareness. Likewise, the ignorance of the regional dimension of cybersecurity could harm the national cohesion, as a cyberattack against the region could be as destructive and costly as an attack against the entire state, with far-reaching repercussions on its economy as well as socio-economic stability. The role of the regions in the EU cybersecurity architecture is paramount.

More specifically, the regional authorities can play an important role in rising cybersecurity awareness among the local SMEs. Representing 99%

of all businesses in the EU and providing two-thirds of the total private sector employment, they are of particular importance to the EU (European Commission, *Entrepreneurship...*, n.d.). Unlike large corporations, SMEs often lack resources or expertise to implement both the digitalisation of their operations and the appropriate cybersecurity measures to protect them. They also too often rule out the possibility of a cyberattack because they assume that they are too small to draw the cybercriminals' attention. The local authorities can effectively address the poor cybersecurity practices by tailored initiatives. The Keep IT Secure (KIS) initiative by Digital Wallonia (Belgium) and Basque Industry 4.0 by the Basque Country (Spain) serve as very good examples. Both programmes have been designed to help local SMEs assess different cybersecurity threats and take the appropriate measures to protect their businesses.

The ignorance of the regional dimension of cybersecurity could harm the national cohesion, as a cyberattack against the region could be as destructive and costly as an attack against the entire state, with far-reaching repercussions on its economy as well as socio-economic stability.

In terms of the EU cybersecurity market development, regions can significantly contribute to the development and deployment of European cybersecurity products and services, thus reducing the EU's reliance on cybersecurity solutions coming from the third countries. Even if the Union has a sufficiently solid cybersecurity landscape with dedicated strategies and financial instruments, it still largely depends on non-European providers. The European regions can play a significant role in escaping this cul-de-sac by leveraging their knowledge of the local cybersecurity ecosystem and adopting national and European resources to solve region-specific challenges. By providing business support to the local cybersecurity SMEs, regions can help to facilitate the commercialisation of European cybersecurity solutions. For example, the Institute for Business Competitiveness of Castilla y León (Spain) has developed a pre-commercial

public procurement programme, which promotes the acquisition of cybersecurity solutions starting with the research, innovation, and development (R&I&D) phase, thus providing the local cybersecurity companies with the financial support and incentives to work on innovation and technological development (ECISO, 2019). For these reasons, regional authorities should be recognised as a thriving force for the digital transformation of the EU.

Regions can significantly contribute to the development and deployment of European cybersecurity products and services, thus reducing the EU's reliance on cybersecurity solutions coming from the third countries.

Finally, the key role of the regions should be recognised not only in the implementation but also in the design of the European cybersecurity programmes. Having a knowledge of the local cybersecurity ecosystem, regions have a great potential to contribute to accelerating the cybersecurity innovation. The cybersecurity research projects would benefit from involving regional representatives. Such involvement would help to ensure the sustainability and applicability of the research projects to market needs. To achieve this, the future European technology research programmes, such as Horizon Europe, would need to clearly integrate the regional dimension and establish practices for more robust involvement of regional research bodies.²

The existing regional cybersecurity initiatives in the EU

The EU has recognised the importance of regions to its cybersecurity posture, and thus economic stability and growth, which reflects at the strategic and policy levels. Unlike its previous version, the updated 2017 cybersecurity strategy, titled *Resilience, Deterrence and Defence: Building strong*

cybersecurity for the EU, stated that the regional dimension of cybersecurity readiness is very important to ensure the EU's readiness to effectively prevent and react to cyber incidents. The document also underlined the importance of facilitating "more targeted capacity building in different regions" (European Commission, 2017). In addition to conferences and tailored workshops to address the role of the regions, few key European initiatives have been launched to support regional cybersecurity building.

The CYBER project has been initiated under the EU Interreg Europe programme and the European Regional Development Fund (ERDF) financial instrument to strengthen the local cybersecurity SMEs and to boost interactions among the European regional cybersecurity ecosystems (Interreg, n.d.). The lack of cooperation among different cybersecurity stakeholders and different ecosystems is identified as one of the challenges preventing local cybersecurity SMEs from scaling up and internationalising their business. The CYBER involves nine institutional partners, representing different EU countries and regions: Bretagne Development Innovation agency (France), Institute for Business Competitiveness of Castilla y León (Spain), Tuscan Region (Italy), Digital Wallonia agency (Belgium), Brittany Region (France), Kosice IT Valley (Slovakia), Chamber of Commerce and Industry of Slovenia (Slovenia), Estonian Information System Authority (Estonia), as well as the European Cyber Security Organisation (Belgium). To address the cooperation challenge, project partners work together to develop and implement regional action plans and concrete policy instruments to improve the inter-regional cooperation.

The European Cyber Valleys pilot project is another EU initiative launched to address regional cybersecurity aspects (European Commission, *Smart...*, n.d.). Just like CYBER, it recognises the interregional cooperation as a key enabler for facilitating the development of the European cybersecurity value chain, reducing market fragmentation, as well as boosting the investment and commercialisation of the European cybersecurity solutions. Currently, the project involves the European regions which

² The involvement of regional research centres to such programmes as the Horizon Europe would allow the actors to better manage the cascade funding for the SMEs to uptake or develop digital innovation, as the regional authorities would be able to serve as intermediaries between the EU funds and the local cybersecurity companies that seek funding.

identify cybersecurity as a strategic smart specialisation priority, namely Estonia and the regions of Castilla y León (Spain), Brittany (France), North Rhine-Westphalia (Germany), and Central Finland (Finland). One activity recently implemented under the European Cyber Valleys framework was the mapping of European regional cybersecurity ecosystems, which helped to identify the European cybersecurity capabilities provided by 470 regional cybersecurity players. The project continues developing the operational strategy which would allow further development of the EU's regional cybersecurity ecosystems, a.k.a. cyber valleys.

The CYBER project and the European Cyber Valleys pilot action are two fine examples of the targeted initiatives aimed to reduce European cybersecurity market fragmentation and to strengthen its competitiveness on a global stage by involving the regions. However, such time-bound initiatives for the regional involvement are not sufficient. The regions should be institutionalised and become a permanent feature of the EU cybersecurity-building efforts. For this, multi-level governance, involving the European, national, and regional levels, should be established.

Multi-level approach to the EU cybersecurity governance

The application of the multi-level governance approach to the EU cybersecurity policy implementation would allow European regions to play an active role in strengthening the EU cybersecurity posture. Multi-level governance is defined as the dispersion of central political power and the delegation of decision-making processes between governments and non-governmental actors at various territorial levels (Bache & Flinders, 2004, p. 3). Due to the ever-evolving risks and far-reaching implications of cybersecurity, the European regions cannot be left in a wait-and-watch position. To establish the effective multi-level governance, the vertical and the horizontal dimensions of regional involvement in the EU's cybersecurity governance should be recognised: responsibility-sharing across different levels of government (i.e. European, national, and regional) as a vertical dimension and inter-regional cooperation as a horizontal dimension.



Placing the European regions next to the EU and the national government as one of the key actors in the EU cybersecurity governance provides a territorial perspective on cybersecurity issues.

The vertical dimension of multi-level governance is important because it allows the European regions to take an active role in the cybersecurity policy formulation and implementation. Placing the European regions next to the EU and the national government as one of the key actors in the EU cybersecurity governance provides a territorial perspective on cybersecurity issues. The European regions are better placed to initiate and coordinate certain types of cybersecurity initiatives. They also possess a more intimate grasp of the cybersecurity developmental needs, on-the-ground policy issues and the state of cybersecurity in their respective territories. By representing regional perspectives, policy efforts undertaken at the regional level can effectively complement pan-European (as well as international) discussions on cybersecurity. Likewise, the regions can help to build awareness of the policy outcomes in their respective territories and be the strategic drivers in the implementation of the internationally agreed decisions.

The cooperation among the regions as the horizontal dimension of multi-level governance is important for its potential to reduce cybersecurity market fragmentation, which remains one of the biggest challenges for the EU. The interregional cooperation helps to break down regional silos and establish trustworthy communication channels which in turns incentivises sharing good practices and exchanging information on the regional challenges and needs. The creation of such linkages between the regions not only can help to optimise the EU's cybersecurity coordination but also benefit the local cybersecurity SMEs. These companies can have more opportunities to scale up their business outside their local market and facilitate the commercialisation of their cybersecurity solutions abroad. The interregional cooperation is also fundamental for developing regional innovation ecosystems, because the less the regions are fragmented, the more they can exploit their cybersecurity innovation potential.

In lieu of conclusions

This article argued that to have a truly effective EU cybersecurity, European regions should be recognised as important players and involved in the policy formulation and implementation. The key strength of the regions is their proximity to the local cybersecurity market players and their familiarity with the local cybersecurity ecosystems. As an intermediate governance level between the national and the European, they can significantly contribute to the enhanced EU's cybersecurity posture in a more effective and sustainable manner. They have instruments to reduce policy overlaps, create synergies among different stakeholder groups, and enhance the innovative performance and commercialisation of European cybersecurity companies.

Despite the regional cybersecurity initiatives fostered by the EU and some clearly successful examples of the local initiatives implemented by the regions themselves, their role is not well recognised. The territorial perspective on the EU cybersecurity policy formulation and implementation is rather rudimental. European regions often find themselves confined to the roles of mere consultation and feedback providers but never rise to the positions associated with negotiations and decision-making.

To take the full advantage of the regions' potential, their role in the EU cybersecurity governance should be institutionalised. The vertical and the horizontal engagement of the regions would help establish the multi-level governance of the EU cybersecurity. To achieve this, responsibility-sharing among the European, national, and regional levels of government and the interregional cooperation mechanisms should become inherent components of the EU cybersecurity governance. ■

CONNECTING EUROPEAN CYBER VALLEYS



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

EUROPEAN CYBER VALLEYS: PILOT ACTION



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



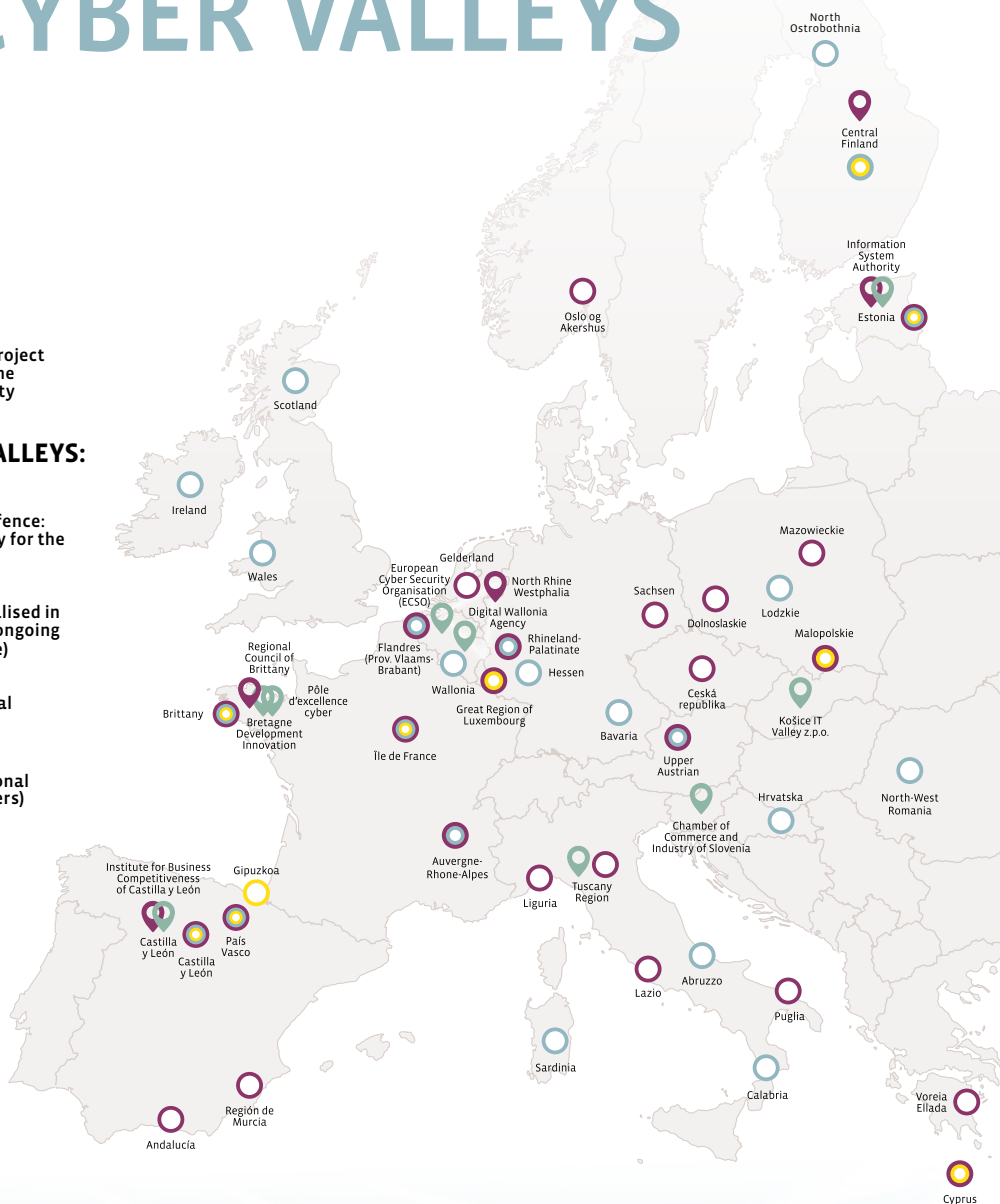
Digital Innovation Hubs specialised in cybersecurity (established or ongoing process based on JRC database)



Smart specialisation or regional strategy on cyber security



ECSO Regional members (Regional authorities and regional clusters)



About the author:



Milda Kaklauskaitė is a Policy Manager at the European Cyber Security Organisation (ECSO). She works on such issues as cybersecurity market analysis and investment promotion, competitiveness and scaling up opportunities for the European cybersecurity startups and SMEs, as well as European regional cooperation on cybersecurity. Before joining ECSO, she worked at the Brussels-based political thinktank, at the Lithuanian Parliament as an assistant to MP and the Lithuania-based communications agency. She holds master's degree in international relations from Central European University (CEU) and bachelor's degree in political science from Vilnius University Institute of International Relations and Political Science (VU IIRPS).

References

Bache, I., & Flinders, M. (2004). Themes and Issues in Multi-level Governance. In Bache, I., & Flinders, M. (Eds.), *Multi-level governance* (pp. 1–11). Oxford/New York: Oxford University Press.

Cimpanu, C. (19 December 2019). Frankfurt shuts down IT network following Emotet infection. ZDNet. Retrieved from <https://www.zdnet.com/article/frankfurt-shuts-down-it-network-following-emotet-infection/>

European Commission. (2013). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001>

European Commission. (5 July 2016). *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2321

European Commission. (2017). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Retrieved from <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450>

European Commission. (n.d.). *Entrepreneurship and Small and medium-sized enterprises (SMEs)*. Retrieved from https://ec.europa.eu/growth/smes_en

European Commission. (n.d.). *Smart Specialisation Platform: Cybersecurity*. Retrieved from <https://s3platform.jrc.ec.europa.eu/cybersecurity>

European Cyber Security Organisation (ECSO). (2019). *The Role of the regions in strengthening the European Union's cybersecurity*. Retrieved from <https://ecs-org.eu/documents/publications/5dc043279c3fd.pdf>

Interreg Europe CYBER. (n.d.). *Regional policies for competitive cybersecurity SMEs: Project summary*. Retrieved from <https://www.interregeurope.eu/cyber/>

Dunn Cavelty, M. and Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing different roles of the state. *St Antony's International Review* 15 (1). 37–57.

Pôle d'excellence cyber. (n.d.). *Présentation du Pôle*. Retrieved from: <https://www.pole-excellence-cyber.org/presentation-du-pole/>

Rouen hospital turns to pen and paper after cyber-attack. (21 November 2019). BBC. Retrieved from <https://www.bbc.com/news/technology-50503841>