The role of the Interreg Programmes in strengthening cyber security within the regions of the Republic of Moldova

Anatolie BABIN,
MBA, Academy of Economic Studies of Moldova
anatolii.babin@ase.md

Sergiu TUTUNARU,
Academy of Economic Studies of Moldova
tutunaru@ase.md

Ion COVALENCO,
Academy of Economic Studies of Moldova
covalenco@ase.md

Abstract
To explore the role of Interreg programmes in strengthening cyber security in the regions of Moldova, which is an increasingly important aspect of national security, especially in regions prone to cyber threats. The work is based on the authors' recent results published in international publications in previous years. The research is based on innovative concepts of digital economy aimed at developing smart villages. Drawing on European experience, accumulated good practices and case studies, the study highlights the importance of international cooperation and capacity building initiatives to reduce cyber risks and build cyber defence capabilities in Moldova. The results of the study highlight the importance of a framework for cross-border cooperation to promote a holistic approach to cybersecurity, integrate best practices and facilitate the sharing of expertise and resources between neighbouring countries. In the context of smart specialisation approaches, digital innovations in rural areas will reach consumers – local action groups – faster, creating synergies between national funds and international programmes at the regional level. Recommendations are made for policy makers, practitioners and stakeholders to further leverage European cross-border programmes to improve cybersecurity resilience and ensure a more secure digital environment in the regions. Implications: academics, researchers, practitioners, EU Commission, JRC. The value of this paper is derived from its examination of the influence of transregional programmes on the advancement of cyber resilience, the facilitation of information sharing, and the stimulation of interregional collaboration. Furthermore, it offers recommendations based on the analysed best practices for addressing cyber security challenges in the context of the specific development of the Republic of Moldova.

Keywords: cybersecurity, interreg, cross-border security operations centers.

1. Introduction
In the context of accelerating digitalization and the growing number and impact of cybersecurity incidents, the European Commission adopted the "EU Cybersecurity Strategy for the Digital Decade" in December 2020. Among other goals, the Cybersecurity Strategy aims to improve capacity and collaboration in detecting cyber threats before they can cause large-scale damage, in order to detect more threats and do so much faster. Russia's incursion into Ukraine further highlights and reinforces the need to urgently build cybersecurity capabilities at the national and Union levels, including through increased information sharing and improved detection of cybersecurity threats to help improve situational awareness and inform preventive and responsive actions.

Cross-border cooperation promotes integrated regional development between neighboring regions having sea and land borders in two or more Member States, or between neighboring regions in, at least, one Member State, and a third country on the external borders of the

Union other than those concerned by the Programs in the field of the Union's external financing instruments [1]. Interreg VI (2021–2027) covers all 27 EU Member States, six accession countries and thirteen neighbouring countries. The participation of Russia in Interreg programmes is suspended following Russia's aggression against Ukraine [2].

The EU Cyber Security Strategy proposes to establish, strengthen and integrate security operations centers (SOCs) and cyber threat intelligence (CTI) capabilities (monitoring, detection and analysis) across the European Union (EU) to support the detection, prevention of cyber threats and timely warning to authorities and all relevant stakeholders' sides. Such cybersecurity capabilities are typically provided by security operations centers (SOCs) of public and private organizations in combination with computer emergency response teams/computer security incident response teams (CERT/CSIRT), supported by external specialized sources of cybersecurity threat intelligence. To implement this strategy, the EU DIGITAL funding program has allocated to "Building the Capacity of Security Operations Centres". One of the key actions envisaged is the creation of cross-border platforms to pool data on cybersecurity threats between multiple Member States.

2. Understanding European Cross-border and Interreg Next Programmes

Cross Border Cooperation (CBC) is a key element of the EU policy towards its neighbours. It supports sustainable development along the EU's external borders, helps reducing differences in living standards and addressing common challenges across these borders.

Territorial cooperation under Interreg is built around four strands [3]:

- Interreg A – cross-border cooperation between adjacent regions (which should in principle be located along land or sea borders separated by up to 150 km of sea) to tackle common challenges identified jointly in the border regions and to exploit the untapped growth potential in these areas.
- Interreg B – transnational cooperation over larger transnational territories or around sea basins with a view to achieving a higher degree of territorial integration.
- Interreg C – interregional cooperation through four specific programmes to boost the effectiveness of cohesion policy by promoting:
    a) The exchange of experiences, innovative approaches and capacity building with a view to identifying and disseminating good practices and implementing them in regional development policies, including the „investment for jobs and growth goal" programmes;
    b) The exchange of experiences, innovative approaches and capacity building with a view to identifying, transferring and capitalising on good practices on integrated and sustainable urban development (the Urbact programme);
    c) The exchange of experiences, innovative approaches and capacity building with a view to improving and simplifying the implementation of Interreg programmes and cooperation actions, along with the setting up and operation of European groupings of territorial cooperation;
    d) The analysis of development trends in relation to territorial cohesion goals the European Spatial Planning Observation Network (ESPON) programm [4].

- Interreg D – cooperation between outermost regions to facilitate the development and integration of outermost regions and OCTs (for example, Caribbean regions) in their neighbouring environment. Interreg NEXT programmes [5] foster cooperation and tackle shared challenges among Member States and non-EU countries from East and South Neighbourhood region of the EU.

Cross-border infrastructure projects are fixed-asset investments that physically link two or more countries via infrastructure, including digital infrastructure, enabling the flow of people, goods, commodities or data [6]. Regional innovation governance refers to all processes of interaction between different actors that together determine the priorities, strategies, activities and outcomes of research and innovation at the regional level. This governance involves adopting institutional arrangements that facilitate systemic interactions between different innovation actors in the region, for example through the triple helix model of innovation or between policy hierarchies with improved policy coordination through multi-level governance.

Multilevel innovation governance [7] can be defined as a complex process of co-operation between different levels of government (supranational, national, regional, local) and/or agents to promote innovation for territorial development strategies. It aims to open up regional innovation strategies, such as the Smart Specialisation Strategy (S3), to other actors in production and knowledge systems simultaneously at different scales. Thus, it is important to implement practices that promote collaboration and alignment across levels of government and territorial entities in defining and developing S3 and other regional strategies to promote more effective multilevel governance. The Partnership for Regional Innovation (PRI) [8] focuses on developing more effective multi-level governance and strengthening synergies between policies and between different funding instruments such as the Cohesion Policy and Horizon Europe, while enhancing stakeholder engagement and co-governance. Encouraging innovative and partnership-based methods of multi-level management [9] of economic, technological and social development is forcing a change in the mentality and practice of populated areas in the regions Republic of Moldova. The Community practices learned should be enriched by innovative and experimental local practices, based on the experience and knowledge of local and regional elected representatives who are most often required to implement common policies and apply Community legislation. In this regard, experimentation is a good governance tool that allows actions to be taken on a small scale to test their impact with a view to wider adoption if the results are convincing, and allows policymakers to base their decisions on evidence that has already been tested at the level of their territorial impact.

2. The Role of Regions in Cross-border Cooperation

European Cross-Border cooperation, known as Interreg A, supports cooperation between NUTS III regions [10] from at least two different Member States lying directly on the borders or adjacent to them. It aims to tackle common challenges identified jointly in the border regions and to exploit the untapped growth potential in border areas, while enhancing the cooperation process for the purposes of the overall harmonious development of the Union. 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 Republic of Moldova to identify their key sectors for generating investment, discovery entrepreneurial potential at the local level 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.

In accordance with the objectives of the Council of Europe Convention No. 106 of May 21, 1980 (concluded in Madrid), cross-border cooperation is understood as any concerted action aimed at strengthening and promoting relations between neighboring territorial communities and authorities under the jurisdiction of two or more Contracting Parties, as well as the conclusion of any agreements and arrangements necessary to achieve the above objectives. Cross-border cooperation is carried out within the powers of territorial communities (Regions) and authorities determined by the internal legislation of each of the Parties. 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 [11], namely:

- 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.

In this context, European Cyber Security Organisation (ECSO) [12] has mapped 25 sustainable local strategies (e.g. Brittany, Central Finland and North Rhine Westphalia, "Connecting European Cyber Valleys"). 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" addressing the emerging challenges posed by cyber security and the increasing digitalisation of the society.

The 2017 EU Joint Communication "Resilience, Deterrence and Defence: Building a strong cyber security for the EU" [13] underlined that cyber security requires a comprehensive cross-policy approach involving the whole economy and all levels of government, including local and regional authorities. The EU strongly promotes the

position that international law, and in particular the UN Charter, applies in cyberspace. As a complement to binding international law, the EU endorses the voluntary non-binding norms, rules and principles of responsible State behaviour that have been articulated by the UN Group of Governmental Experts it also encourages the development and implementation of regional confidence building measures [14], both in the Organisation for Security and Co-operation in Europe and other regions.

3. Multi-level Governance in Cybersecurity

Regions 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 National government are not enough and that more structured inclusion of the regional and local authorities to the definition of they strategic role and needs in cybersecurity in the way to integration in Digital Single Market of EU. Therefore, we argue that the multi-level governance model needs to be established to include regions Republic of Moldova in the EU cybersecurity policy implementation. One of the principal advantages of regional entities is their proximity and capacity to cultivate trust among cybersecurity stakeholders at a local level. Unlike national governments, whose vantage point is often constrained by the necessity of maintaining a comprehensive overview of the nation's cybersecurity posture, regions enjoy more proximate connections with local cybersecurity stakeholders, encompassing a range of actors, including end users, integrators, research and innovation (R&I) centers, and product and service providers. The French Ministry of Armed Forces and the Brittany Region launched a noteworthy initiative, the "Pole d'excellence cyber", to enhance the country's cyber resilience through a collaborative approach with regional authorities on cybersecurity matters. This initiative exemplifies a state's potential to benefit from regional expertise in cybersecurity. It also underscores the value of regional involvement in cybersecurity innovation and industry development, especially when these issues are challenging to address by national authorities due to their limited understanding of regional cybersecurity contexts and dynamics.

The Governments of the Republic of Moldova and the French Republic concluded March 7, 2024 in Paris an agreement on cooperation in the field of defense. The document comes in the context of strengthening bilateral cooperation relations and adjusting the legal framework to the current security situation [15]. In frameworks of Partnerships for Regional Innovation (PRI), there is four main pillars when developing multi-level governance:

- Complexity (dealing with conflicts);
- Emergence (learning through the process);
- Context specificity (different regional experiences);
- Reciprocity (recognising each other level of governance).

Like large companies and administrations, the Ministry of the Armed Forces has launched its digital transformation which should enable it to offer 100% digitalized business processes (dematerialized services) and to have a suitable digital ecosystem with the expectations of its employees and partners. Defined within the Digital Ambition of the Armed Forces, the objectives of the digital transformation of the Armed Forces are to:

- Guarantee operational superiority and control of information in theaters of operation;
- Strengthen the efficiency of support and facilitate the daily lives of staff;
- Improve the relationship with citizens and the attractiveness of the ministry.

Broken down into broad guidelines, these objectives aim in particular to develop an innovation ecosystem as well as the use of emerging technologies for the benefit of the ministry's systems and applications. By choosing a strong technological transformation, the ministry offers itself the possibility of becoming a leading digital player.

If new information technologies [16], as shown in the Figure 1, allow companies to have certain competitive advantages, they can also allow the Armed Forces to benefit from a primordial operational advantage.

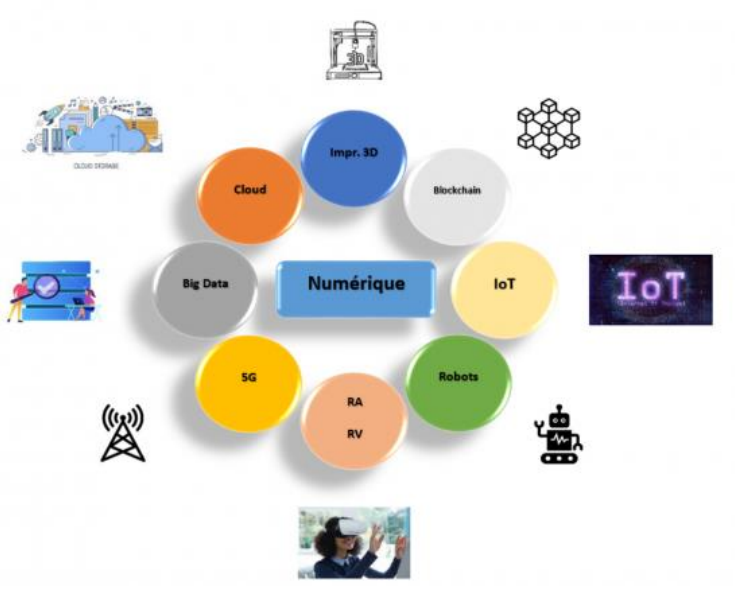

Fig. 1. Overview of innovative technologies.

AI can, for example, pilot aircraft systems supported by combat drones (SCAF), data analysis using Big Data techniques can help identify areas for improvement in our operational functioning, the cloud secure which can make it possible to have operational data available at any time and in any place within extremely short deadlines, autonomous robots can carry out risky tasks for humans (e.g.: mine clearance), the blockchain can immutably store sensitive data from our activity while ensuring their total traceability.
The European Network of Defence-related Regions (ENDR) was created in 2016 by the European Commission. The ENDR has three objectives [17]:

- Bringing regional organisations and clusters together to exchange best practices on how to develop dual use (defence-related) development strategies, including the integration of defence industrial and research assets into smart specialisation strategies, and support defence-related SMEs;

- Facilitating the flow of information about funding opportunities (such as the European Defence Fund and European Structural and Investment Funds); and
- Promoting the development of regional clusters of excellence.

One of the best EU practicies in frameworks of this network, which present a role of regions in Multi-level Governance, can be „European Cluster of Ceramics", that operate at the regional, national, european and international levels. The mission of the European Cluster of Ceramics is to boost the activity of the ceramics sector through innovation. Thus, it animates its network to increase its capacity:

- Accelerate innovation thanks to the active support of the engineering team;
- Boost growth through networking and visibility activities;
- Dvelop business on the European and international scale.

The "Association for the development and promotion of the European ceramic center" also known as European Cluster of Ceramics is a competitiveness cluster specialised in ceramics and related materials and processes. The cluster represents 119 manufacturers, 36 laboratories and 5 RTOs from France, Portugal, Switzerland, Belgium, Italy, and Germany. The cluster is part of other associations including ERMA (European Raw Material Advanced) and Cerame-Unie. Furthermore, the European Ceramic Cluster actively participates and influences the regional roadmap on advanced materials. With the aim of fostering innovation within its sector, the cluster's strategy is defined around four strategic markets:

- Luxury and Design (Tableware, jewelry, cosmetic);
- Energy systems (Mechanical components, buildings and refractories);
- Electronics, Electrical and optical components;
- Protection of people and environment (bioceramics, filters, armouring).

In the field of dual applications, the defence cluster covers high-performance materials such as transparent ceramics for ballistic defence and aeronautical applications, surface treatment, etc. The objective of the cluster is to facilitate collaborative R&D projects across the three components, Figure 2, which will bring together companies, public research laboratories and academic institutions in order to create new products and services on the market.

Fig. 2. Three Transitions in Innovation Ecosystem of "European Cluster of Ceramics".
Source: https://cerameurop.com/en/the-cluster/

Additionally, the cluster aspires to assist enterprises in the advancement of their innovation and to stimulate their economic development, particularly with regards to the export sector. In this regard, the Sirena'Mic project, financed by the Nouvelle Aquitaine region, represents a significant avenue for ceramic companies. This programme is specifically designed to facilitate the expansion of these enterprises into international markets, with a particular focus on the aeronautics, space and defence sectors in Europe and the USA, among other regions.

Republic of Moldova is a new candidate country and member of Interreg Europe programme. In this context multi-level innovation governance can be an important topic for many Interreg Europe projects, with partipation regions and local authoroties. As an example of building multi-level governance in regions and between them, can be among which: ECORIS3, aiming to foster policies and measures to support local and regional innovation ecosystems; RELOS3 which promotes the deployment of S3 at the local level; S34GROWTH that aims to enhance interregional collaboration through new industrial value chains; COHES3ION integrating a regional and sub-regional element into S3 and looking into how regions can develop their multi-level governance [7]. The Orkestra Basque Institute of Competitiveness shared six insights on multi-level governance:

- The urgency of developing multi-level governance;
- Its systemic nature (responding to complexity);
- The need for a new role for citizens in multi-level governance;
- The apparent dilemma between efficiency and democratisation;
- The importance of complementarities and collaboration in multi-level-governance;
- The hybrid nature of multi-level governance (responding to its emergent nature).

4. Strategies for Effective Cross-border Cooperation

Cross Border Cooperation (CBC) is a key element of the EU policy towards its neighbours. It supports sustainable development along the EU's external borders, helps reducing differences in living standards and addressing common challenges across these borders.

The developed overall strategy for sustainable management of the transboundary area between Bulgaria and Romania within the framework of the SPATIAL [18] project aims at a common integrated approach to solving development problems in the border areas of neighboring countries, overcoming the limitations imposed by national borders. Taking a holistic approach and taking into account economic, social and environmental elements, the strategic nature of the project is emphasized by the proposed activities:

- Identification of local capacity within the framework of S3 approaches;
- Identification of key issues/industry areas of analysis;
- Development of an integrated and harmonized database of border settlements of neighboring countries;
- Development of a strategy covering transboundary territory;
- Finding ways of cooperation between authorities and citizens, as well as between all interested parties in border areas;

- A unified approach to the implementation of investment projects within the framework of the Danube Strategy of the European Union and the European Structural and Investment Funds for the period.

The SPATIAL project has defined and established a framework interoperability Web-GIS systems, Fugure 3, for cooperation to facilitate the use of potential capital/local assets of the border areas of the countries in order to increase competitiveness and innovation along the entire common border, as well as to protect and improve the environment in the context of the development priorities of the European Union.

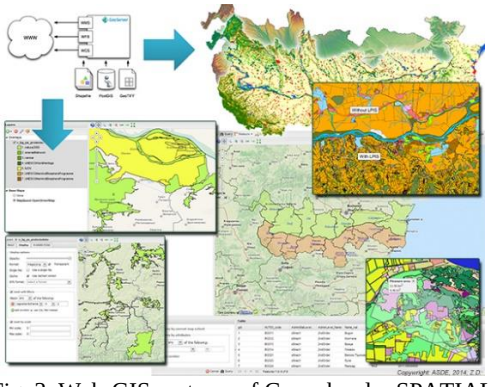

Fig. 3. Web-GIS systems of Cross-border SPATIAL
Source: https://cbc171.asde-bg.org/

B-solutions [19] is a pilot initiative aimed at removing legal and administrative border barriers along the EU's internal land borders. This initiative could well complement the methodology of the SPATIAL project, if it is adapted to the section of the Moldavian-Ukrainian and Moldavian-Romanian borders, within the framework of one project. B-solutions is promoted by the European Commission's Directorate-General for Regional and Urban Policy (DG REGIO) and managed by the Association of European Border Regions (AEBR) as one of the actions proposed in the Communication "Boosting growth and cohesion in EU border regions". The fundamental objective of b-solutions is to identify and implement solutions to legal and administrative border obstacles [20]. This entails enabling border-adjacent municipalities and regions, as well as cross-border entities, to submit information about border-related legal or administrative obstacles they face. Successful candidates are then assigned support from the European Commission to remove these border-related obstacles. In this new context for the Republic of Moldova, as an EU candidate country, we highlight the best practices of neighboring countries in the joint planning "Common Strategy for Sustainable Territorial Development of the Romania-Bulgaria Border Territory".

In our publications [21], we have repeatedly emphasized the role of Living Labs, the concept of which effectively contributes to the innovative development of settlements and organizations participating in its functioning. Living Labs are open innovation ecosystems in real-world settings that use iterative feedback processes throughout the innovation lifecycle to ensure sustainable impact. They focus on co-creation, rapid prototyping and

testing, and scaling innovation and business by delivering (various types of) shared value to stakeholders. In this context, living laboratories can also act as intermediaries/organizers between citizens, research organizations, companies and government agencies of border areas and Euroregions. The "European Parliament resolution of 15 September 2022 on EU border regions: living laboratories of European integration" [22] welcomes the 2021 Commission communication [23] which places emphasis on the following cooperation topics [24]:

- Barriers faced by EU border regions;
- Specific characteristics of border regions;
- Sustainability through closer institutional cooperation;
- More and better cross-border government services;
- Dynamic cross-border labor markets;
- Border regions for the European Green Deal.

In accordance with the Council Conclusions on the EU's Cyber Posture of May 2022 and as previously announced in the Joint Cyber Defence Communication, the Commission has proposed the EU Cyber Solidarity Act [25]. This Act encompasses a series of measures designed to reinforce solidarity and enhance coordinated EU detection and situational awareness. At the same time, it aims to bolster Member States' preparedness and response capabilities to significant or large-scale cybersecurity incidents. This is achieved through [26]:

- The European Cyber Shield will comprise a pan-European infrastructure of Security Operation Centers (SOCs), which will be utilized to construct and enhance coordinated detection and situational awareness capabilities;
- The Cybersecurity Emergency Mechanism will be employed to provide support to Member States in the preparation for and response to major or large-scale cybersecurity incidents;
- The Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents;
- The European Cyber Shield will consist of a pan-European infrastructure that connects Security Operations Centres (SOCs) spread across the EU.

Procedure for creating a cross-border SOC platform [27] with funding support are follow:

- Following a request for expressions of interest, the European Commission will select applicants intending to establish a cross-border SOC platform;
- All parties to the request nominate their national coordinators, with whom the European Cybersecurity Competence Center (ECCC) [28] enters into a joint agreement for deployment and use, for example in border areas. This agreement sets out practical arrangements for managing the deployment and use of tools and infrastructure jointly owned by the ECCC and participating national SOCs following joint procurement. The coordinator is usually the national SOC of one of the EU Member States participating in the consortium;
- Each selected coordinator will participate in joint procurement of goods and services with ECCC;

- Individually participating partners in each selected consortium may apply for an additional grant to cover eligible costs such as the creation and launch of a cross-border SOC platform.

The EU contribution will cover up to 75% of the cost of purchasing instruments and infrastructures. The remaining procurement costs will be covered by the member states participating in each cross-border SOC platform. The ECCC Financial Rules set out the conditions under which the ECCC may engage in procurement, including joint procurement with member states.

A technical group, composed of experts from EU Member States, has been created to support the process and, in particular, to help identify the main types of goods and services that need to be jointly procured and to discuss the overall plan at a high level. Typical examples of procured goods and services identified by the technical team include (indicatively):

- Hardware: servers, micro data center racks, high-speed switches, firewall switches, GPUs, HSMs, sensors;
- Software: visualization tools, SIEM tools, vulnerability managers, aggregation tools, incident reporting tools, situation awareness correlation tools, AI/ML tools, PKI tools, orchestration systems;
- Services: CTI channels, AI/ML feature updates, dedicated virtual phone line, cloud storage, software development and customization services, consulting services.

The goal is to promote convergence between different platforms and, to the extent possible, to use procurement to acquire goods and services that can benefit all platforms. If properly justified, procurement may also include specific types of goods and services for individual platforms.

5. Policy Recommendations:

- One of the principal objectives of the "Initiating cross-border and interregional cooperation" initiative is to identify the characteristics and key services that a cross-border innovation ecosystem designed to support Small and Medium-sized Enterprises (SMEs) in the cybersecurity sector should provide.
- For potential partner public administrations, it is advisable to focus on identifying the main barriers to success. These include a lack of coordination between relevant actors, market fragmentation, and a lack of skills. For each identified barrier, a SWOT analysis should identify the strengths, weaknesses, opportunities, and threats at the regional and cross-border levels.
- In light of the varying levels of cyber development among partners, it is recommended that they identify best practices that align with their respective strengths and potential solutions to the needs of other partners. The European best practices identified in the article can be classified into two distinct categories of policies that facilitate multi-level governance of cyber defense. The first category encompasses policies that support the structure of the cyber innovation ecosystem, while the second category encompasses policies that support the advanced services

provided within the ecosystem. Examples of the latter category include labeling, access to public and private funding, capacity building, and so forth.

- As a consequence of inter-regional exchange processes, partners are able to select and adapt best practices and solutions, which are then reflected in regional Action Plans. The Action Plans serve to provide a concrete and tangible roadmap for interested regional authorities, delineating a pathway through which they may develop and channel greater levels of funding in order to enhance the competitiveness of SMEs in the field of cybersecurity. Moreover, their relevance is crucial in the context of Moldova's EU integration, as they provide a contribution that can be made to the European Investment for Growth and Jobs Program and the European Territorial Cooperation Program. Additionally, they can be utilized to address cybersecurity issues through the lens of the recently proposed NIS2 Directive. The aforementioned cross-border action plans, developed by the partners, serve as pivotal documents for both regional cooperation in Europe and for policy.

6. Conclusions

Regions can play a pivotal role in the advancement and dissemination of cybersecurity products and services in Europe, reducing the EU's dependence on third-country and non-European solutions. The near-future European cybersecurity landscape will be influenced by initiatives with a direct impact on regional ecosystems, including the European Cybersecurity Competence Centre Network, European digital innovation hubs, and the renewed smart specialization strategy in each region. Consequently, interregional collaboration is of paramount importance for the identification of solutions and the advancement of a more integrated cybersecurity market. 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 should be 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 Regional Technology Offices, training centres, services operators, incubators, SMEs and assist to establishe clusters initiatives and large companies.
- Regional level should be significant in disseminating good practices and establishing preventive measures and immediate response services due to its proximity with the end-users.
- Regions should play a 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 should be the direct users of cyber security products when developing their sectoral policies (e.g. health, energy or transport).

The Cross-border SOC platforms must enable and encourage the exchange and consolidation of large volumes of cybersecurity threat data from multiple sources in a trusted environment, and provide high quality, actionable information to their members through expert analysis and the use of state of the art information modern tools and

infrastructure. This should serve to improve detection capabilities and ultimately prevent and respond to cyber threats and incidents.

References

[1] European Commission, "Directorate-General for EU regional and urban policy," May 2024. [Online]. Available: https://ec.europa.eu/regional_policy/policy/cooperation/european-territorial/cross-border_en# .

[2] TESIM, "Neighbourhood External Cooperation Programmes Interreg VI (2021–2027)," EU, 2024. [Online]. Available: https://interregtesimnext.eu/about-interreg-next/ .

[3] EUR-lex, "Interreg – Supporting cooperation across borders" (2021–2027)," [Online]. Available: https://eur-lex.europa.eu/EN/legal-content/summary/interreg-supporting-cooperation-across-borders-2021-2027.html .

[4] European Commission, "European Observation Network for Territorial Development and Cohesion (ESPON)," [Online]. Available: https://www.espon.eu/espon-2030/espon-2030-programme.

[5] European Commission, "Directorate-General for EU regional and urban policy," [Online]. Available: https://ec.europa.eu/regional_policy/policy/cooperation/european-territorial/next_en.

[6] European Invest Bank, "Cross-border infrastructure projects," May 2023. [Online]. Available: https://www.eib.org/en/publications/20230107-cross-border-infrastructure-projects .

[7] Interreg Europe, "Multi-level Governance for Innovation," 24 January 2023. [Online]. Available: https://www.interregeurope.eu/find-policy-solutions/stories/multi-level-governance-for-innovation.

[8] European Commission, "Partnerships for Regional Innovation: 63 regions, seven cities and four Member States selected for Pilot Action," 17 May 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3008.

[9] EUR-lex, "Encouraging innovative and partnership-based methods of governance," Publications Office of the European Union, 2024. [Online]. Available: lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52009IR0089.

[10] European Commission, "Interreg A - Cross-border cooperation," Directorate-General for EU regional and urban policy, [Online]. Available: https://ec.europa.eu/regional_policy/policy/cooperation/european-territorial/cross-border_en .

[11] EU Network EUROBITS, "The Role of the Regions in strenghtening the European Unionțs cyber security Position Paper," 15 March 2019. [Online]. Available: https://www.eurobits.de/wp-content/uploads/20190320_Regions_Position_Paper_approved.pdf.

[12] European Cyber Security Organisation (ECSO), "ECSO to lead ECCO, the European Cybersecurity Community Support project," 20 December 2022. [Online]. Available: https://ecs-org.eu/ecso-to-lead-ecco-the-european-cybersecurity-community-support-project/.

[13] European Commission, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU," 2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450.

[14] CCDCOE, "OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection," [Online]. Available: https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/ .

[15] Republic of Moldova, Minisrty of Defence, "Intergovernmental Defense Cooperation Agreement signed in Paris," 7 March 2024. [Online]. Available: https://www.army.md/?lng=3&action=show&cat=122&obj=8847 .

[16] Ministry of Defence of France , "Digital transformation in the Army," [Online]. Available: https://www.defense.gouv.fr/terre/nos-materiels-nos-innovations/nos-innovations/pole-numerique-coordination-linnovation/numerique-0# .

[17] "The European Network of Defence-related Regions (ENDR)," [Online]. Available: https://endr.eu/about-us/ .

[18] Agency of Sustainable Development and Eurointegration – Ecoregions (ASDE), "Common Strategy for Sustainable Territorial Development of the cross-border area Romania-Bulgaria 2012-2014," [Online]. Available: https://cbc171.asde-bg.org/ .

[19] Association of European Border Regions (AEBR), "b-solutions," January 2022. [Online]. Available: https://www.aebr.eu/projects/b-solutions/ .

[20] Association of European Border Regions (AEBR), "b-solutions," [Online]. Available: https://www.b-solutionsproject.com/about.

[21] A. A. Babin, I. V. Covalenco, S. A. Tutunaru and E. A. Babina, "Some Aspects of the Formation of an Innovation Ecosystem for the Sustainable Development of Smart Villages in the Republic of Moldova," *INstrumentul Bibliometric Național,* p. 52, 2023.

[22] European Parliament, "European Parliament resolution of 15 September 2022 on EU border regions: living labs of European integration (2021/2202(INI))," 15 September 2022. [Online]. Available: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0327_EN.html.

[23] European Commission, "EU Border Regions: Living labs of European integration," Brussels, 2021.

[24] European Commission, "Delivering the European Green Deal," 14 July 2021. [Online]. Available: https://commission.europa.eu/publications/delivering-european-green-deal_en .

[25] European Commission, "Commission welcomes political agreement on Cyber Solidarity Act," 6 March 2024. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1332.

[26] European Commission, "A European Cyber Shield to step up our collective resilience | Opening of the International Cybersecurity Forum | Speech by Commissioner Thierry Breton," 5 April 2023. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2145 .

[27] European Commission, "Cybersecurity: EU launches first phase of deployment of the European infrastructure of cross-border security operations centres," 24 November 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-launches-first-phase-deployment-european-infrastructure-cross-border-security .

[28] European Commission, "Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres," 20 May 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0887.