BUILDING EUROPE'S CIVILIAN-DEFENCE CYBER RESILIENCE THROUGH EXPANDING AND CONSOLIDATING NETWORKS: THE ECYBRIDGE EXPERIENCE

Niculae IANCU[1], Maria-Mihaela GURĂU[2], Gabriel RAICU[1], Marilena-Jeana CÎMPINEANU[2]
[1] Maritime Cybersecurity Centre of Exellence, Constanța Maritime University, Constanța, Romania
nicu.iancu@marcyscoe.org, gabriel.raicu@marcyscoe.org
[2] Research, Analysis and Training Department, Euro-Atlantic Resilience Centre, Bucharest, Romania
maria.gurau@e-arc.ro, jeni.cimpineanu@e-arc.ro

Abstract: This article examines the dynamics of network expansion and consolidation in strengthening European cyber resilience, using the ECYBRIDGE initiative as a case study. ECYBRIDGE connects public and private actors from civilian and military sectors, fostering synergies as these networks grow and consolidate. The discussion situates the EU cybersecurity architecture within the conceptual frameworks of multi-level and polycentric governance theory, showing how overlapping decision centres and transnational cooperation can reinforce cyber resilience. Quantitative indicators trace the project's network expansion, while qualitative evidence highlights standardisation and trust-building as hallmarks of consolidation. Four analytical axes organise the analysis: thematic domains of intervention, governance and operational layers, strategic relevance and urgency, and integration challenges with enabling mechanisms. Taken together, these findings demonstrate how the progressive expansion and consolidation of such networks enhance Europe's cyber resilience and point towards more robust, inclusive, and interoperable models of cybersecurity governance.
Keywords: ECYBRIDGE, cyber resilience, civil-military cooperation, multi-level governance, polycentric governance.

INTRODUCTION

The ECYBRIDGE project is a pioneering European Union initiative funded through the Digital Europe Programme and implemented by a multinational consortium of 17 organisations, with oversight provided by under the European Cybersecurity Competence Centre (ECCC). It is designed to foster coherence and interoperability across Europe's cybersecurity landscape by building bridges between civilian and defence communities, including both public and private actors. This article uses ECYBRIDGE as a theory-informed case study to examine how networks for cyber resilience expand and, crucially, how they consolidate through standardisation and trust-building. It mobilises concepts from network theory, multi-level governance (MLG), and polycentric governance to explain why certain governance configurations are better suited to addressing Europe's rapidly evolving and cross-sectoral cyber risks.

While Europe has accelerated the expansion of cybersecurity networks, expansion alone does not guarantee resilience. We advance the central hypothesis that *European cyber resilience improves when the expansion of stakeholder networks is matched by consolidation through standardisation and trust-building, under a blended governance architecture that combines the institutional coherence of multi-level governance with the adaptive capacity*

of polycentric arrangements. In short: expansion without consolidation yields coordination gaps; consolidation without breadth risks insularity; the optimal pathway is a sequenced and mutually reinforcing combination of both, situated in an MLG–polycentric hybrid.

Our argument proceeds in three steps. Firstly, drawing on Manuel Castells' conception of networks as dynamic, reconfigurable sets of nodes, we specify how network expansion (more nodes, ties, and information flows) creates both opportunities (reach, redundancy, innovation) and vulnerabilities (coordination costs, variable capacity). Secondly, we theorise consolidation as the emergence of shared standards, interoperable procedures, and trust-based information exchange, outcomes that reduce transaction costs and enable coordinated action at scale. Third, we locate these dynamics within a governance architecture. MLG provides vertical alignment and formal authority across EU–national–sectoral levels; polycentric governance supplies horizontal adaptiveness through overlapping, semi-autonomous centres capable of experimentation and rapid mutual adjustment. The expectation is that where expansion and consolidation co-evolve within this blended architecture, resilience gains become observable and durable.

Methodologically, the article employs a mixed-methods design. Quantitative indicators from ECYBRIDGE track network expansion (e.g., growth in participating organisations and geographies, cross-sector engagement, interaction density across events). Qualitative evidence, derived from tabletop exercises, foresight workshops, academic roundtables, high-level policy dialogues, and policy recommendations, identifies consolidation mechanisms, notably standardisation processes and trust-building practices (shared taxonomies, incident-reporting routines, proto-doctrinal alignment, training initiatives and liaison roles). Triangulation across activity streams strengthens inference regarding causal mechanisms linking governance design to resilience outcomes.

To structure the interpretation, findings are organised along four analytical axes: thematic domains of intervention; governance and operational layers; strategic relevance and urgency; and integration challenges and enabling mechanisms. This framework allows us to trace how similar problems, such as intelligence-sharing deficits or technological asymmetries, manifest across domains and layers, and how enabling mechanisms (communities of practice, boundary organisations, joint simulations) translate into consolidation.

The article offers three contributions. Theoretically, it articulates how MLG and polycentric logics function as complements in European cyber governance. Empirically, it provides project-based evidence that standardisation and trust-building are the distinctive signatures of consolidation that make expanded networks operationally meaningful. Policymaking-wise, it outlines practicable pathways for interoperable, inclusive governance models, linking EU-level ambition to national implementation and cross-sector execution. The conclusion returns to the hypothesis and shows how the ECYBRIDGE case supports it: resilience improves where expansion is paired with consolidation within a blended MLG–polycentric architecture particularly relevant in the European Union context, and it outlines policy steps to institutionalise that blend.

NETWORK DYNAMICS: EXPANSION AND CONSOLIDATION

Building on the research hypothesis, this section conceptualises networks as the foundational architecture of cyber resilience and specifies the dual processes of expansion and consolidation

that shape their evolution. The aim is to explain why growing the number of connections alone does not guarantee resilience unless those connections are stabilised through shared standards, trust, and the capacity for coordinated action. Network theory provides the analytical lens through which these dynamics are first examined before turning to the governance frameworks that can sustain them.

Castells (2004, p. 3) defines a network as "a set of interconnected nodes", whose significance lies not in the intrinsic attributes of any single node but in its capacity to sustain and direct information flows in pursuit of collective objectives. Nodes increase their importance by "absorbing more relevant information and processing it more efficiently", while those unable to add value become marginal and are eventually "deleted" as the network reconfigures itself. This conception foregrounds three properties that are particularly relevant for cybersecurity governance: dynamism, because networks continuously adapt to shifting flows of data; relational power, because influence derives from the ability to connect, filter, or block information rather than from fixed hierarchies; and self-regeneration, because redundant elements are reduced and new ones incorporated. Figure 1 illustrates this conceptualisation by mapping the network's core components and the relationships through which information flows and influence emerge.

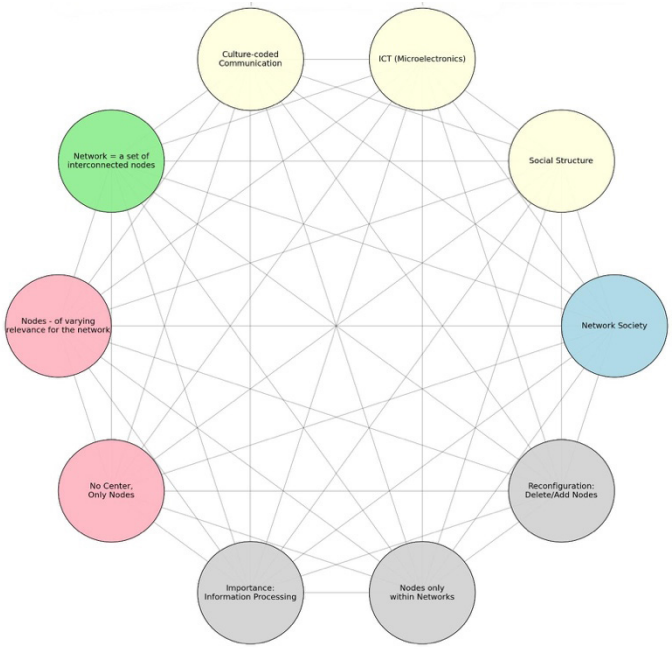

Figure 1. Conceptual representation of network nodes and interconnections
(Illustrating information flows, dynamic reconfiguration, and the position of influential nodes.)

As shown in Figure 1, a network's structure is defined less by the intrinsic qualities of individual nodes than by the density and direction of the connections among them, a feature that enables both the expansion and consolidation processes analysed below. These properties make networks powerful engines of expansion. They grow by adding nodes and increasing the density of their interconnections, distributing influence across a wide array of actors and reducing vulnerability to the failure of any single component. Yet the same features also create the need for consolidation. Without mechanisms of trust-building, standardisation, and

shared situational awareness, expansion can lead to fragmentation and coordination failure. The tension between these two tendencies, openness and stabilization, lies at the heart of the ECYBRIDGE inquiry and provides the conceptual link to the governance discussion that follows.

A defining feature of networked systems is their decentralisation. Without a single centre of power or control, authority and influence are distributed across nodes. This property underpins network expansion, allowing new participants to join and information flows to multiply without requiring the consent of a central authority. It also renders networks less vulnerable to collapse, as no single point of failure can disable the entire system. In cybersecurity, this explains both the robustness of the internet's core architecture and the rapid growth of multi-stakeholder coalitions that share threat intelligence across borders.

Yet, as Castells (2004; 2009) reminds us, the diffusion of authority does not mean that power disappears; it is reconfigured. Influence resides in the ability to connect, disconnect, and filter information flows. Nodes that can aggregate, amplify, or block data, such as major technology platforms, critical infrastructure operators, or state cyber agencies, acquire disproportionate weight. For cyber governance this means that even in ostensibly horizontal structures, pivotal actors emerge whose strategic position allows them to set de facto standards and shape collective outcomes. Expansion therefore brings with it an implicit need for consolidation, so that such asymmetries are channelled into legitimate and transparent decision-making.

Decentralisation also generates distinctive exclusion dynamics. Although networks are adaptive and open-ended, not all actors can participate on equal terms. Access to resources, technological capacity and digital literacy determines who can integrate and how effectively they can contribute. Nodes that fail to add value are eventually "deleted", creating new axis of inequality between the "networked" and the "non-networked". In cyber governance this can marginalise smaller organisational actors, under-resourced agencies or SMEs, reinforcing the need for integrative mechanisms, including standards, funding instruments and communities of practice, that promote inclusive consolidation as networks expand.

Equally significant is the self-regenerative quality of networks, which makes them highly adaptable. They can reroute information, recruit new participants or modify their structure when confronted with disruption. This property explains both the resilience of decentralised digital infrastructures and the ability of transnational movements, such as Occupy, #MeToo and the Arab Spring, to mobilise rapidly without centralised leadership. At the same time, it enables the persistence of harmful formations, including disinformation ecosystems or extremist groups, that resist suppression. Effective consolidation in cybersecurity must therefore strike a balance: preserving the adaptive benefits of regeneration while curbing its potential to reproduce malicious actors.

A final, cross-cutting dimension is unpredictability inherent in organically evolving networks. Influence can arise from unexpected nodes. For example, a small social media account that suddenly becomes globally significant. Because networks evolve in response to changing information flows, they are difficult to forecast or control. This volatility might be regarded as a source of creativity. Decentralised exchanges of knowledge foster the rapid development of new ideas, technologies, and social movements that might never emerge in more rigid, hierarchical systems. Yet the very unpredictability that fuels innovation also creates systemic

risks. Disinformation campaigns, cascading cyberattacks, or the sudden amplification of extremist voices can proliferate with a speed and scale that outstrip traditional oversight. Networks therefore inhabit a paradoxical space, functioning simultaneously as engines of progress and as vectors of instability, and highlighting why consolidation mechanisms, such as early-warning systems, real-time information sharing, and jointly rehearsed response protocols, are indispensable factors to expansion.

Taken together, these dynamics show that network growth is not a simple matter of scaling up. Expansion and consolidation must advance in tandem if Europe's cyber resilience is to keep pace with the rapidly increasing number of cybersecurity actors, including public authorities, defence organisations, private companies, research institutes, and specialised start-ups, that populate today's digital security landscape. Decentralisation, power reconfiguration, exclusion pressures, regenerative capacity, and unpredictability all create opportunities for innovation and resilience but also vulnerabilities that can only be mitigated through structured trust-building, standardisation, and interoperable technical platforms**.** ECYBRIDGE directly addresses this challenge by bringing together diverse civilian and defence stakeholders through cooperative mechanisms such as cross-sector exercises, joint foresight workshops, and dedicated digital infrastructures for secure information exchange. This conceptual insight leads naturally to the next step in the analysis: identifying governance models capable of sustaining this delicate equilibrium. Multi-level governance provides the institutional architecture for coherence across jurisdictions, while polycentric governance supplies the adaptive capacity for continuous learning and rapid mutual adjustment. The following section elaborates these complementary frameworks and shows how they illuminate the ECYBRIDGE case.

MULTI-LEVEL GOVERNANCE AND POLYCENTRIC GOVERNANCE OF THE CYBERSPACE

Multi-level governance

Multi-level governance (MLG) provides a foundational lens for understanding how authority is organised and exercised in the European cyber domain. In contrast to state-centric models that presume a neat separation between domestic and international politics, MLG highlights the vertical dispersion of decision-making across local, national, regional, supranational, and global levels, as well as the horizontal interdependence among them.

Highly cited theorists Liesbet Hooghe and Gary Marks emphasise that, in an MLG system, "decision-making competencies are shared by actors at different levels rather than monopolised by national governments" and that collective decision-making among states entails a "significant loss of control for individual national governments" (Hooghe & Marks, 2001). They further stress that political arenas are interconnected rather than nested, so that national governments function as nodes in a wider web of governance, no longer serving as the sole interface between supranational and subnational arenas.

A key conceptual refinement introduced by Hooghe and Marks is the distinction between Type I and Type II multi-level governance. Type I refers to stable, general-purpose jurisdictions, such as the European Union, its member states, and regional authorities, while Type II captures flexible, task-specific arrangements such as agencies, regulatory networks, and transnational partnerships. This typology is highly relevant for cybersecurity. Type I structures (e.g., the

European Commission, ENISA, or national cybersecurity agencies) offer formal authority and legal coherence, but they struggle to keep pace with the borderless and rapidly changing digital environment. Type II structures (e.g., Computer Emergency Response Teams, Cyber Defence Commands, cross-border public–private partnerships, and specialised EU initiatives such as ECYBRIDGE) provide the flexibility needed for real-time threat detection, information sharing, and joint operational response.

Adding a further conceptual layer, Anne Mette Kjær (2004) argues that governance should be understood as intrinsically layered, encompassing everything from local administrative networks to supranational and global systems. Although she does not address digital governance directly, her approach enables a conceptual leap highly pertinent to cyberspace: authority in this domain is exercised through overlapping institutionalised layers, from local-level digital strategies and national cybersecurity plans to EU-wide directives such as GDPR and NIS2, and even global norm-setting forums. Kjær's emphasis on governance networks and the hollowing-out of centralised authority underscores that digital governance is not unidirectional but is continually shaped by interaction among diverse and dispersed actors operating across multiple scales.

The analytical value of multi-level governance in the European context lies in its ability to reveal both opportunities and tensions. On the one hand, MLG provides mechanisms for aligning strategies, harmonising regulatory standards, and pooling resources across borders. On the other, it highlights the risks of implementation gaps and vertical misalignments, where EU-level ambitions are only partially translated into national operational plans or where local actors lack the capacity to meet European norms. By making these frictions explicit, MLG helps identify where additional coordination, capacity-building, and legal integration are required.

Polycentric governance

The concept of polycentric governance was first articulated by Vincent Ostrom, Charles Tiebout, and Robert Warren in their seminal 1961 article *"The Organization of Government in Metropolitan Areas,"* where they challenged hierarchical models of public administration by showing how overlapping jurisdictions could foster more responsive and efficient governance. Vincent Ostrom later refined this idea, defining a polycentric political system as one in which "many officials and decision structures are assigned limited and relatively autonomous prerogatives to determine, enforce and alter legal relationships" (Ostrom 1999: 55). This formulation emphasizes that polycentricity entails not just multiple authorities, but overlapping and relatively autonomous centers of decision-making that enable flexibility, mutual adjustment, and innovation outside a monocentric chain of command. Building on these foundations, Elinor Ostrom extended the concept to the global level in her 2010 article *"Polycentric Systems for Coping with Collective Action and Global Environmental Change,"* where she argued that polycentric arrangements are better suited to complex, cross-scale challenges such as climate change because they encourage experimentation, learning, and redundancy. Taken together, these contributions highlight polycentric governance as both a structural and functional response to complexity—an insight highly relevant to cybersecurity, where overlapping authorities at local, national, regional, and global levels must constantly adapt to evolving, borderless threats in the digital domain.

"Standing on the shoulders of the titans" and building directly on Vincent and Elinor Ostrom's foundational work, McGinnis (2016) develops polycentric governance as both an aspirational ideal and a set of practical limitations. The Ostroms emphasized that overlapping centers of authority, if allowed to make mutual adjustments, could foster experimentation, adaptability, and resilience in governing complex systems. McGinnis extends this framework by distinguishing between the ideal-typical vision of polycentricity and the realities of practice, identifying recurring traps such as coordination failures, inequities, and excessive complexity that undermine governance performance. Yet, he argues that polycentric systems retain built-in mechanisms for learning and recalibration, echoing Elinor Ostrom's insistence on nested, adaptive arrangements. This synthesis is particularly useful for analyzing cybersecurity, where authority is dispersed across local, national, regional, and global levels, and where both the promise of adaptive governance and the pitfalls of fragmentation are acutely visible.

As McGinnis (2016) synthesizes from the Ostrom tradition, "a polycentric system of governance consists of (1) multiple centers of decision-making authority with overlapping jurisdictions (2) which interact through a process of mutual adjustment during which they frequently establish new formal collaborations or informal commitments, and (3) their interactions generate a regularized pattern of overarching social order which captures efficiencies of scale at all levels of aggregation, including providing a secure foundation for democratic self-governance."

Despite its clear practical relevance, polycentric governance in cybersecurity remains under-theorized due to a combination of structural, disciplinary, and political factors. Cybersecurity itself is a fast-moving domain, driven by technological innovation and urgent crises that often outpace conceptual reflection, while scholarship continues to rely heavily on state-centric paradigms that obscure the decentralized, multi-actor dynamics of practice. In reality, much of cybersecurity governance is already polycentric, with private companies, platform security teams, and CERTs leading responses, but these practices rarely feed into theory-building. Efforts at conceptual integration are further hampered by disciplinary silos, methodological challenges in measuring complex and often opaque governance systems, and the political sensitivities of attribution, sovereignty, and public–private power relations. Unlike in environmental studies, where Elinor Ostrom's framework has become influential, cyber studies have yet to fully embrace its insights, leaving a theoretical vacuum. At the same time, this gap offers an opportunity: advancing polycentric governance theory in cybersecurity could provide tools that better reflect the distributed, adaptive, and multistakeholder realities of this critical domain.

In this respect, acknowledging that "while interconnectivity within cyber space increases efficiency, it reduces resilience to cyber-attacks", Masato Kikuchi and Takao Okubo propose using polycentric governance as means of building resilience in cyber space.

The essence of cyberspace lies in its decentralized architecture of interconnections, which imparts an anarchic quality to the domain. As David Clark has emphasized, cyberspace is not created by individual computers but by the interconnections that span all its layers, producing a system without a single center of authority. In Castells' terms, these networks embody a "space of flows," where the logic of inclusion and exclusion is determined by informational connectivity rather than territorial boundaries. Such anarchic connections resonate with the

Ostromian notion of polycentricity, in which multiple autonomous centers of decision-making coexist and adjust to one another without hierarchical command. Yet cyberspace is not a realm of pure anarchy: its apparent disorder is tempered by overlapping governance mechanisms rather stemming from multi-level governance, such as protocols, standards bodies, states, and private actors, that continuously negotiate order within a polycentric system.

Complementary models

The complementarity of multi-level and polycentric governance is increasingly recognised in cybersecurity studies. Multi-level governance, grounded in enduring, nested institutional structures, provides the formal architecture and legitimacy of governance, while polycentric governance adds adaptive flexibility by enabling semi-autonomous actors to coordinate, innovate, and respond rapidly to emerging threats. The theoretical basis for this duality lies in Hooghe and Marks's typology of MLG, which distinguishes between stable jurisdictions (Type I) and overlapping, task-specific networks (Type II).

Furthermore, in its report Multi-level Governance Reforms. Overview of OECD Country Experiences, the OECD (2017) highlights that multi-level governance reforms work best when combined with cross-sectoral and flexible coordination mechanisms. In cybersecurity, this means vertical alignment (states, EU, international frameworks) coupled with horizontal cooperation (public-private partnerships, CERTs, industry consortia).

Taken together, these perspectives lend support to the metaphor of multi-level governance as the skeleton and polycentric governance as the nervous system of cyber governance, combining institutional coherence with resilience and adaptability.

The following section applies these theoretical insights to the case of a Digital Europe grant, *Strengthening Synergies in Defence and Civilian Cybersecurity* (ECYBRIDGE), analyzing the first year of its ongoing 24-month implementation in order to illustrate how multi-level and polycentric governance dynamics manifest in practice.

INSIGHTS FROM ECYBRIDGE

Building a Unified European Cybersecurity Architecture with ECYBRIDGE

Strategically situated at the intersection of civilian and defence cybersecurity domains, the ECYBRIDGE project exemplifies a broader paradigm shift in the governance of cyber resilience, one that unsettles the historically entrenched separation between military and civilian spheres. Traditionally, defence institutions handled high-end deterrence and national security, while civilian agencies were responsible for infrastructure protection and digital services (Dunn Cavelty, 2008). More recently, however, security thinking has undergone a profound epistemic transformation, marked by processes of diffusion and constructed societalisation, whereby concepts such as risk, vulnerability, and resilience are no longer framed exclusively in relation to external threats but are increasingly understood as constitutive dimensions of embedded socio-technical systems. This shift is eloquently elaborated by Dunn Cavelty (2024), who demonstrates how the security discourse has expanded inward to encompass societal vulnerabilities, crisis preparedness, and continuous risk management through technologies such as surveillance systems and algorithmic

governance, transforming cybersecurity into an everyday enterprise of governance rather than an exceptional wartime response.

This reconceptualisation is especially salient in cyberspace, where hybrid threat vectors exploit interdependencies across critical infrastructures and civilian–military interfaces, rendering strictly sectoral approaches insufficient (Kello, 2013; Klimburg, 2012). Accordingly, resilience has shifted from a sector-bounded posture to a systemic, networked understanding emphasising adaptability, redundancy, and the rapid restoration of essential functions (Linkov et al., 2013). Operationally, this has foregrounded interoperability, trust-building, and shared situational awareness as the linchpins of effective civil–military cooperation, features that are characteristic of polycentric and multilevel governance arrangements capable of coordinating diverse centres of decision-making under conditions of uncertainty (Ansell & Gash, 2008; Boin & Lodge, 2016; Ostrom, 2010). Within the European Union, these shifts cohere with an explicit policy trajectory that seeks to develop cross-sector cyber capacities as part of a broader project of strategic autonomy and collective resilience, including in the digital space (Christou, 2016; Carrapico & Barrinha, 2018). Against this backdrop, ECYBRIDGE is best conceptualised not merely as an institutional innovation, but as the practical enactment of this theoretical realignment in cyber governance. It redefines civilian and defence preparedness as mutually constitutive elements within an integrated resilience regime, and systematically operationalises this premise through a diverse array of instruments, including multi-stakeholder policy dialogues, cross-sector academic and professional deliberations, threat-based exercises, and experimental governance mechanisms.

In this context, ECYBRIDGE advances a forward-looking, systems-oriented framework designed to transcend fragmented national responses in favour of a unified and resilient European cybersecurity architecture. Anchored in the evolving regulatory infrastructure of the European Union, as for example the *NIS2 Directive*, the *Cyber Resilience Act*, and the *EU Cybersecurity Act*, the project seeks to operationalise the EU's ambition for strategic autonomy in the digital domain. Rather than functioning solely within the confines of technical compliance, ECYBRIDGE embodies a governance logic rooted in multi-level and cross-sectoral collaboration, bringing together actors from civilian, military, academic, and private-sector domains. This co-production of strategic knowledge and capability development represents a 360-degree contribution to the advancement of Europe's cyber resilience, with particular emphasis on institutional alignment, procedural coherence, and network-style visibility across stakeholder communities.

The scope of ECYBRIDGE is both conceptually ambitious and methodologically diverse, encompassing a suite of interrelated activities aimed at catalysing institutional transformation and consolidating cross-sector cybersecurity networks across Europe. During its first year of implementation, the project initiated a series of foundational undertakings designed to foster institutional learning, promote multi-actor engagement, and advance operational integration. A core component of these efforts was a threat-based tabletop exercise simulating cyberattacks on dual-use infrastructures. This scenario-based simulation provided a controlled environment to assess coordination mechanisms, test the interoperability of civilian and defence actors, and identify procedural and communicative bottlenecks. In addition to reinforcing the importance of shared situational awareness, the exercise illuminated persistent structural gaps,

underscoring the urgent need for policy harmonisation, capacity-building, and standardised response protocols to ensure collective readiness in real-world crisis scenarios.

Building upon this operational foundation, ECYBRIDGE also convened strategic foresight workshops that drew on cybersecurity lessons from the Ukrainian conflict. These sessions applied structured analytical tools, most notably STEEP and PESTLE, to anticipate future technological disruptions, institutional asymmetries, and resilience deficits in an increasingly volatile and hybrid threat environment. These policy–technology hybrid activities offered a forward-looking lens to explore systemic vulnerabilities and plausible future scenarios, thereby informing both capability development and policy alignment across national and sectoral boundaries.

In parallel, the project facilitated a series of academic roundtables and high-level policy dialogues, enabling knowledge exchange among research institutions, public authorities, and operational stakeholders. These deliberative spaces fostered critical reflection on governance gaps, strategic priorities, and regulatory fragmentation, while simultaneously advancing a shared understanding of civilian-defence cyber convergence. These cumulative initiatives culminated in ECYBRIDGE's flagship event, *Navigating Cyber Storms: Civilian and Defence Synergy in a Digitalised World*, an international conference that served as a high-level platform for synthesis, dissemination, and stakeholder engagement. By convening a diverse array of actors from across the cybersecurity spectrum, the event reinforced the project's integrative and multidimensional approach to advancing European cybersecurity governance.

These interventions ultimately converged in the publication of a comprehensive White Paper, which articulates a governance model for civil–defence cyber convergence in the European Union. Synthesising insights from operational exercises, foresight analyses, and multilateral dialogues, the document outlines concrete institutional, legal, and technical pathways for enhancing cyber interoperability, strategic coordination, and cross-sector trust. Through its integrative methodology and sustained outreach, ECYBRIDGE has helped shape a nascent epistemic community around cyber resilience, one committed to collaborative policy innovation and shared preparedness. In doing so, the project aligns with, and substantively contributes to, the European Union's broader strategic agenda of reinforcing digital sovereignty, embedding anticipatory governance, and cultivating robust response capabilities in an era defined by systemic uncertainty and hybrid threats.

Interpreting ECYBRIDGE's Empirical Findings: A Layered Analysis of Cyber Resilience Synergies Within the EU Cybersecurity Landscape

This section provides a structured and conceptually informed interpretation of the empirical contributions generated through the ECYBRIDGE project. Rather than treating the project's outputs as discrete activities or deliverables, the analysis applies a multidimensional interpretive framework that categorises key findings across four interrelated axes: (1) thematic domains of intervention, (2) governance and operational layers, (3) strategic relevance and urgency, and (4) integration challenges and enabling mechanisms. This analytical architecture enables a move beyond descriptive mapping toward a more explanatory assessment of how civil–military synergies and institutional interdependencies are evolving within the broader EU cybersecurity governance framework.

Methodologically, the analysis draws on qualitative content analysis of project deliverables, stakeholder consultations, and communication outputs, triangulated across workshops, tabletop exercises, conferences, and policy dialogues. This empirical corpus facilitates the identification of recurrent patterns, critical deficits, and systemic innovations that define the ECYBRIDGE approach. The aim is not only to clarify what the project has produced, but to explicate how its integrative actions have catalysed institutional learning, encouraged normative convergence, and contributed to the operationalisation of cyber resilience through emerging practices of polycentric governance in the European Union.

Thematic Domains of Intervention

Several interrelated thematic domains emerged as central to the reconfiguration of cybersecurity governance across the European Union. These domains reflect not only the diversity of risks and institutional configurations engaged by the project but also the complex terrain of vulnerabilities, interdependencies, and governance inconsistencies that characterise the EU's evolving cyber ecosystem. Rather than approaching cyber resilience as a static or purely technical challenge, ECYBRIDGE has foregrounded systemic deficits, ranging from policy misalignment to interoperability gaps, that impede the formation of a coherent and inclusive cybersecurity framework.

One recurring thematic domain was the insufficient alignment between civilian and defence cybersecurity frameworks at both strategic and operational levels. Despite the growing interpenetration of digital infrastructures and the rise of hybrid threats targeting dual-use systems, the findings underscore persistent fragmentation in institutional mandates, legal standards, and information-sharing protocols. The lack of common threat taxonomies and joint operational protocols among civilian and military cybersecurity actors was repeatedly flagged as a barrier to coordinated response, with particular urgency attached to the absence of trusted mechanisms for real-time intelligence exchange. These findings resonate with the broader literature on cybersecurity governance, which identifies siloed security cultures and bureaucratic fragmentation as structural impediments to effective resilience, as asserted by Carrapico & Barrinha (2018) and Christou (2016).

A second critical domain concerns the technological disparities and gaps in cyber readiness across Member States and institutional actors. ECYBRIDGE stakeholders emphasised the uneven diffusion of advanced detection, response, and risk mitigation tools, particularly among local authorities, SMEs, and civilian infrastructure operators. The inability to access or integrate cutting-edge solutions, such as automated threat intelligence platforms, cyber range testing environments, and interoperable situational awareness dashboards, was not only seen as a technical issue but as a strategic fault line within the EU's broader cyber defence posture. These challenges are compounded by market asymmetries and procurement bottlenecks, which tend to privilege large, well-resourced actors and reinforce dependency on non-EU technologies, thus undermining the goal of European digital sovereignty.

The third thematic domain relates to normative fragmentation and the absence of binding standards for cross-sectoral cyber crisis management. While several EU-level instruments, such as the NIS2 Directive and the Cyber Resilience Act, offer regulatory support, ECYBRIDGE participants consistently noted gaps in national implementation, enforcement, and sectoral compliance. This incoherence translates into difficulties in operationalising shared resilience

objectives, particularly in cross-border scenarios where attribution, escalation control, and legal interoperability remain contested. The need for harmonised certification, incident reporting protocols, and common strategic foresight mechanisms was repeatedly highlighted as essential for building a resilient digital single market.

Finally, ECYBRIDGE initiatives surfaced the importance of cultural and cognitive domains often neglected in cybersecurity interventions. Participants pointed to the need for cultivating a common strategic culture across civil and military institutions, one that recognises cyber resilience not as the exclusive domain of technical experts but as a multi-actor, multi-level process rooted in trust, communication, and shared situational awareness. This extends to the epistemic communities involved in cyber governance, including academic researchers, think tanks, training providers, and civil society actors. By promoting inclusive deliberative spaces, such as academic roundtables and hybrid foresight events, ECYBRIDGE has begun to reshape the contours of what constitutes legitimate knowledge and authority in cybersecurity policy design.

Taken together, these thematic domains reveal the multifaceted character of the EU's cyber resilience deficit. They demonstrate that enhancing cyber governance requires not merely technological investment or regulatory updates, but a systemic reordering of institutional relationships, shared norms, and operational interoperability. In this regard, ECYBRIDGE has laid the groundwork for a more integrated and polycentric approach to cybersecurity governance in Europe, one that is responsive to strategic challenges, grounded in empirical insight, and attentive to the political complexity of cross-sectoral cooperation.

Governance and Operational Layers

The second analytical dimension through which ECYBRIDGE's findings may be interpreted centres on the governance and operational layers that shape the EU's cybersecurity architecture. These layers, spanning both horizontal (civil-military, public-private, cross-sectoral) and vertical (local, national, supranational) configurations, reveal the institutional density and complexity within which cybersecurity policy and practice unfold in Europe. All ECYBRIDGE's activities consistently exposed key fault lines across and within these layers, while also identifying mechanisms through which interlayer coordination might be improved.

A recurring insight concerned the vertical misalignment between national cybersecurity strategies and EU-level regulatory frameworks. While the NIS2 Directive, the Cyber Resilience Act, and the EU Cybersecurity Act collectively articulate a robust regulatory vision, their translation into national operational plans remains uneven. Several project participants flagged delays or inconsistencies in the transposition of EU directives, resulting in an implementation gap that weakens the EU's collective cyber posture. In particular, the limited integration of national defence planning into EU-level cyber scenarios was cited as a critical vulnerability, especially given the growing convergence of cyber and kinetic threat vectors in hybrid warfare contexts. This highlights the persistent tension between the EU's normative ambition for strategic autonomy and the sovereignty-sensitive nature of security and defence policy among Member States.

At the horizontal level, ECYBRIDGE findings point to substantial coordination deficits between civilian and military cybersecurity actors. Despite increasing rhetorical commitments to cross-

sector cooperation, operational integration remains limited by cultural divergence, asymmetric resource allocation, and institutional compartmentalisation. Notably, ECYBRIDGE's tabletop exercise revealed fragmented chains of command, restricted information-sharing arrangements, and divergent response protocols between civilian emergency management agencies and defence counterparts. This not only impairs incident response efficacy but also limits joint situational awareness, which is essential for crisis escalation management and post-incident recovery. The lack of structured inter-ministerial liaison bodies or shared cyber crisis cells was cited as a recurrent obstacle, reinforcing the need for formalised civil-defence coordination architectures.

Moreover, the governance landscape is further complicated by the proliferation of non-state actors operating across these layers. Private-sector cybersecurity providers, critical infrastructure operators, academic institutions, and think tanks all occupy significant positions within the operational cybersecurity landscape. However, ECYBRIDGE findings suggest that their role remains largely ad hoc, with limited institutionalised pathways for sustained policy engagement. While some Member States have established public-private partnerships or innovation sandboxes, these remain uneven and often under-resourced, particularly in comparison to defence-led initiatives. ECYBRIDGE has addressed this by facilitating deliberative spaces, such as roundtables and stakeholder webinars, that begin to close this gap, but systemic institutionalisation remains an unmet priority.

Finally, the supranational governance layer, primarily embodied by the European Commission, ENISA, the European Defence Agency, and EU-funding programmes, was seen as increasingly pivotal but still lacking enforcement authority in operational matters. ECYBRIDGE's outputs demonstrate that while EU-level institutions are indispensable in agenda-setting, funding, and norm diffusion, their operational footprint is contingent upon the political will and bureaucratic capacity of national authorities. This layered asymmetry underscores the need for stronger coordination mechanisms, more binding compliance instruments, and co-funding arrangements that incentivise joint capability development across Member States.

In sum, the ECYBRIDGE project elucidates the intricate layering of governance and operations that structure European cybersecurity. The interplay between fragmented vertical authority and insufficient horizontal coordination generates vulnerabilities that cannot be resolved through technical fixes alone. What is required is an institutional redesign that embraces polycentric governance: one that allocates responsibilities according to function and expertise, ensures redundancy without duplication, and fosters sustained interaction among civilian, military, and non-state actors. ECYBRIDGE's empirical work not only makes this diagnosis explicit but also offers embryonic models of how such redesign can be operationalised through joint foresight, scenario-based exercises, and multi-actor governance innovation.

Strategic Relevance and Urgency

The third interpretive axis concerns the strategic relevance and urgency of the challenges and opportunities surfaced through ECYBRIDGE's integrated activities. In an increasingly contested digital landscape, where hybrid threats, cyber coercion, and infrastructure interdependencies escalate both in frequency and severity, ECYBRIDGE's empirical insights offer a timely and policy-relevant contribution to the EU's strategic cyber posture. Rather than merely cataloguing technical vulnerabilities or institutional inefficiencies, the project

foregrounds the need to recalibrate European cyber resilience according to differentiated strategic priorities, some urgent and foundational, others systemic and long-term.

Among the most pressing issues identified throughout the ECYBRIDGE hands-on evens was the chronic underdevelopment of trust-based information sharing across the civil–military divide. Although the EU Cybersecurity Strategy and related policy frameworks stress the importance of cross-sectoral trust and collaboration, the reality remains one of limited interoperability and guarded institutional cultures. The inability to rapidly exchange classified or near-real-time operational intelligence between civilian and defence authorities was repeatedly cited as a core inhibitor of effective cyber crisis management. This gap becomes especially critical during cyber-enabled geopolitical escalations, as seen in the Ukrainian context, where the temporal compression of attacks demands accelerated decision-making grounded in joint situational awareness.

In parallel, the project highlighted the high strategic relevance of aligning cybersecurity foresight with national and EU-level defence planning. The emergence of new threat vectors, such as AI-enabled intrusion techniques, supply-chain vulnerabilities, and state-sponsored disinformation campaigns, requires anticipatory rather than reactive frameworks. ECYBRIDGE's use of scenario planning and strategic foresight methodologies revealed that while technical agencies are relatively well-equipped for risk scanning, their outputs often fail to penetrate the strategic decision-making circuits of national security and defence actors. Bridging this divide is not a matter of procedural adjustment but of strategic integration, one that recognises cybersecurity as both a national security imperative and a societal resilience challenge.

Furthermore, ECYBRIDGE findings suggest that EU institutions face a dual burden in the current cybersecurity architecture. On one hand, they are expected to provide normative leadership, technical guidance, and funding incentives for Member States. On the other hand, they must navigate persistent resistance from national actors wary of ceding sovereign control over security prerogatives, notably within the military realm. The strategic urgency of overcoming this impasse is clear. Without a shared sense of purpose and layered responsibility, Europe's cybersecurity will remain fragmented and vulnerable.

Importantly, the project also registered emerging windows of strategic opportunity. The convergence of civilian and defence agendas under the 2022 EU Strategic Compass provides a fertile institutional setting in which cyber resilience can be pursued as a genuinely shared objective. ECYBRIDGE leveraged this moment by exploring a vision of digital sovereignty rooted in capability development, cross-sectoral knowledge production, and multilevel governance integration. This approach reflects the growing consensus that strategic autonomy in the cyber domain is not merely a technological or industrial question, but a governance challenge requiring novel institutional arrangements and a recalibration of strategic priorities.

Consequently, ECYBRIDGE's empirical outputs underscore a dual dynamic in the European cybersecurity landscape: a set of vulnerabilities and coordination failures that demand urgent remediation, and a constellation of institutional innovations and strategic alignments that signal real potential for transformation. By identifying and analysing these tensions, the project contributes to an evidence-based understanding of what constitutes strategic relevance and urgency in today's hybrid threat environment, not only diagnosing Europe's cyber resilience gaps, but also outlining plausible trajectories for systemic reinforcement.

Integration Challenges and Enabling Mechanisms

The final analytical axis concerns the structural and procedural conditions that either inhibit or enable deeper integration across the civilian and defence components of Europe's cybersecurity architecture. ECYBRIDGE's empirical corpus reveals that while policy discourse increasingly favours convergence and coherence, the operational realities on the ground are shaped by institutional inertia, asymmetric capabilities, and governance fragmentation. These integration challenges, however, do not exist in a vacuum. The project's findings also point to a set of emerging mechanisms, both formal and informal, that can facilitate gradual convergence and interoperability across sectors and jurisdictions.

A recurrent obstacle identified through ECYBRIDGE's foresight activities and stakeholder dialogues is the enduring segmentation of cyber responsibilities among national institutions, particularly between ministries of defence, interior, digital affairs, and intelligence agencies. This institutional dispersion not only hampers coordinated responses to cyber incidents, but also generates incompatible terminologies, divergent strategic cultures, and disconnected risk assessment methodologies. The absence of formalised frameworks for information sharing, particularly in relation to classified or threat-intelligence data, further compounds the challenge. In this context, the absence of a shared operational vocabulary and harmonised standards emerges as both a symptom and a cause of fragmentation.

Yet, alongside these challenges, ECYBRIDGE has identified enabling mechanisms that hold promise for institutional adaptation. One such mechanism lies in the establishment of structured communities of practice that cut across institutional boundaries. The project's roundtables, foresight workshops, and the Navigating Cyber Storms conference fostered precisely such ecosystems, where civilian, military, academic, and private-sector actors could jointly articulate threat perceptions, test policy assumptions, and simulate collaborative responses. These deliberative platforms function not merely as forums for exchange, but as proto-institutional infrastructures that cultivate trust, align conceptual frameworks, and prototype governance models.

Another enabling mechanism identified by the project is the mobilisation of intermediary actors, particularly those operating at the intersection of sectors, universities, think tanks, cybersecurity centres of excellence, and public-private partnerships. These entities act as boundary organisations that translate policy into practice, mediate between strategic and operational levels, and build cross-sectoral legitimacy. ECYBRIDGE itself, as a project situated at this intersection, illustrates how such intermediary functions can be institutionalised and scaled to support broader integration objectives.

However, integration remains a contingent and contested process. The path forward requires not only technical interoperability but also political will, normative alignment, and capacity-building. ECYBRIDGE's findings make clear that the success of enabling mechanisms depends on sustained engagement, iterative learning, and the institutionalisation of cross-sector collaboration beyond the lifespan of EU-funded projects. In this sense, integration should not be seen as a fixed endpoint, but as an evolving process that requires constant recalibration in response to shifting threat landscapes, technological change, and geopolitical volatility.

Thus, ECYBRIDGE's exploration of integration challenges and enabling mechanisms reveals a complex terrain marked by both structural constraints and emergent opportunities. Through its empirical work, the project has not only mapped the barriers to civil–military cyber convergence but also helped to prototype feasible pathways for overcoming them, offering a conceptual and practical toolkit for operationalising cyber resilience in a multilayered European security environment.

Cross-Cutting Issues

In interpreting the ECYBRIDGE project's empirical contributions through this four-dimensional analytical framework, it becomes clear that the axes delineated by this study are not mutually exclusive. Rather, they represent intersecting vantage points, different perspectives or angles of analysis that overlap and interact with one another, from which to understand the evolving logic of cybersecurity cooperation in the European Union, as depicted in Table 1.

Table 1. Intersecting vantage points across ECYBRIDGE analytical axes

Cross-Cutting Issue	Thematic Domains of Intervention	Governance and Operational Layers	Strategic Relevance and Urgency	Integration Challenges and Enabling Mechanisms
Civil–military intelligence sharing	Lack of shared threat taxonomies and real-time protocols	Fragmented institutional mandates and vertical asymmetries	High-priority vulnerability in hybrid crises	Absence of secure information-sharing frameworks; need for liaison structures
Technological asymmetries	Gaps in access to advanced tools, especially for SMEs and local actors	Unequal resource allocation across Member States and sectors	Weakening of digital sovereignty and collective defence posture	Potential for joint procurement and capability-building networks
Normative fragmentation	Variability in NIS2 and CRA implementation across sectors and borders	Misaligned legal frameworks between national and EU levels	Strategic incoherence undermines coordinated response	Harmonisation mechanisms, shared certification and reporting standards
Strategic foresight alignment	-	Disconnect between technical foresight and national security planning	Delay in anticipating AI threats, supply-chain risks	Boundary-spanning roles for foresight actors and policy translators
Institutional trust and shared culture	Cultural divergence between civilian and defence actors	Weak inter-agency communication and training	Trust deficit delays response time in crises	Creation of communities of practice; intermediary facilitation roles
Operational interoperability	Emphasis on scenario-based testing and joint simulations	Asymmetric response protocols and fragmented chains of command	Critical for time-sensitive incidents (e.g., kinetic–cyber nexus)	Simulation-based learning and joint operational doctrine development
Private and non-state actor involvement	Inclusion of academia, think tanks, and cybersecurity SMEs	Ad hoc role in policymaking and operational activities	Opportunity to enhance innovation and response diversity	Institutionalising public–private partnerships and cross-sector engagement platforms

As the findings consistently demonstrate, recurrent issues such as intelligence fragmentation, technological asymmetries, or the need for trust-based interoperability do not confine themselves neatly within a single dimension. For example, the lack of civil–military intelligence-sharing simultaneously reflects a thematic policy gap, a cross-layer governance asymmetry, a high-priority strategic vulnerability, and an integration barrier of both normative and technical nature. In this sense, ECYBRIDGE's added value lies not only in its capacity to surface these issues but also in its ability to trace their manifestations across multiple

domains, reinforcing the need for holistic and multi-level approaches to cyber resilience. By situating the project's outputs within this layered analytical schema, we not only move beyond descriptive reporting but offer a structured, conceptually rigorous interpretation of how civilian–defence synergies can be mobilised to meet the challenges of Europe's contested digital future.

CONCLUSION AND THE WAY FORWARD

Even though still an ongoing initiative, ECYBRIDGE has already revealed with clarity that Europe's cyber resilience depends on the twin dynamics of network expansion and consolidation embedded in a governance architecture that combines multi-level and polycentric logics. The project demonstrates that expansion through the rapid proliferation of cybersecurity actors, cross-border initiatives, and knowledge-sharing platforms creates opportunities for innovation and redundancy, yet at the same time generates new vulnerabilities. Consolidation, through trust-based information sharing, standardisation, and the institutionalisation of cross-sector cooperation, converts these opportunities into durable and operational resilience. Crucially, neither dimension is sufficient on its own: expansion without consolidation risks fragmentation, while consolidation without continued growth can lead to insularity and stagnation.

This insight carries significant implications for the future evolution of European cybersecurity governance. Strengthening resilience will require governance models that deliberately weave together the structural coherence of multi-level governance with the adaptive flexibility of polycentric arrangements. Such a blended architecture can secure the benefits of vertical alignment, from EU legislation such as NIS2 and the Cyber Resilience Act down to national and institutional practice, while simultaneously empowering diverse actors to innovate, experiment, and coordinate horizontally across civilian and defence domains. ECYBRIDGE illustrates how this can be achieved in practice by cultivating cross-border trust networks, piloting dedicated technical platforms for secure data exchange, and fostering communities of practice that bridge public and private, civil, and military, academic and operational constituencies.

Looking ahead, the project's experience points to a European cybersecurity strategy in which network growth and consolidation proceed in tandem as a continuous process. EU-level frameworks need to embed incentives for joint capability development and to reinforce implementation mechanisms that ensure regulatory commitments translate into interoperable operational routines. At the same time, investment in distributed nodes of governance, ranging from national and sectoral Computer Emergency Response Teams both civilian and defence to research-driven innovation clusters, must be sustained so that adaptation keeps pace with technological and geopolitical change. By demonstrating how these elements can be aligned and mutually reinforcing, ECYBRIDGE provides a template for the next generation of EU cybersecurity initiatives, helping to transform a complex and fragmented landscape into a genuinely integrated and anticipatory European cyber resilience regime.

REFERENCE LIST

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. Journal of Public Administration Research and Theory, Volume 18, Issue 4, October 2008, Pages 543–571.

Boin, A., & Lodge, M. (2016). Designing resilient institutions for transboundary crisis management: A time for public administration. Public Administration, 94(2), 289–298.

Carrapico, H., & Barrinha, A. (2018). European Union cyber security as an emerging research and policy field. European Politics and Society, 19(3), 299–312.

Castells, M. (2004). Informationalism, networks, and the network society: A theoretical blueprint. In M. Castells (Ed.), The network society: A cross-cultural perspective (pp. 3–45). Edward Elgar.

Castells, M. (2009). Communication Power. Oxford University Press.

Christou, G. (2016). Cybersecurity in the European Union: Resilience and adaptability in governance policy. Palgrave Macmillan.

Clark, D. D. (2010). Characterizing cyberspace: Past, present and future. MIT Communications Futures Program Report. Massachusetts Institute of Technology.

Dunn Cavelty, M. (2008). Cyber-security and threat politics: US efforts to secure the information age. Routledge.

Dunn Cavelty, M. (2024). The politics of cybersecurity. Routledge.

European Commission. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L333, 80–152.

European Commission. (2023). Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). COM(2022) 454 final.

Hooghe, L., & Marks, G. (2001). Multi-level governance and European integration. Rowman & Littlefield.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. International Security, 38(2), 7–40.

Kikuchi, M., & Okubo, T. (2020). Building cyber resilience through polycentric governance. Journal of Communications, 15(5), 390–397.

Kjær, A. M. (2004). Governance. Polity Press.

Klimburg, A. (Ed.). (2012). National cyber security framework manual. NATO Cooperative Cyber Defence Centre of Excellence.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476.

McGinnis, M. D. (2016). Polycentric governance in theory and practice: Dimensions of aspiration and practical limitations. Policy Studies Journal, 44(1), 36–58.

Organisation for Economic Co-operation and Development (OECD). (2017). Multi-level governance reforms: Overview of OECD country experiences. OECD Publishing.

Ostrom, E. (2010). Polycentric systems for coping with collective action and global environmental change. Global Environmental Change, 20(4), 550–557.

Ostrom, V. (1999). Polycentricity (Part 1). In M. D. McGinnis (Ed.), Polycentricity and local public economies: Readings from the Workshop in Political Theory and Policy Analysis (pp. 55–74). University of Michigan Press.

Ostrom, V., Tiebout, C. M., & Warren, R. (1961). The organization of government in metropolitan areas: A theoretical inquiry. American Political Science Review, 55(4), 831–842.

Niculae IANCU is vice-president of the Maritime Cybersecurity Centre of Excellence at the Constanta Maritime University. With a career spanning over thirty years, he has accumulated significant experience in international military cooperation, and strategic planning in security and defence, and possesses profound knowledge of NATO and EU policies. His expertise also includes defence and security research, as well as teaching security and intelligence in higher education settings. Previously serving as the Rector of the National Intelligence Academy in Bucharest, Romania, Dr. Iancu now lectures on security and strategic studies, diplomacy and global affairs, cybersecurity policy and risk management at various European universities.

Maria Mihaela GURĂU (née Nistor) works at the Department of Research, Analysis and Training at the Euro-Atlantic Resilience Centre, under the Romanian Ministry of Foreign Affairs. Her expertise covers emerging and disruptive technologies, societal resilience, and geopolitics. She has served as general director within the Ministry of Education, visiting lecturer at Babeș-Bolyai University, expert in EU-funded projects, invited speaker and seminar leader at George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen. She holds a PhD in International Relations and Security Studies (summa cum laude, Babeș-Bolyai University, 2015), two MAs in International Relations and German Studies, and BAs in Philology and Political Sciences. Her academic path includes scholarships at Universität Leipzig, Universitat Rovira i Virgili, and Queen's University, Canada.

Gabriel RAICU is the Rector of Constanta Maritime University (CMU) and President of the Maritime Cybersecurity Centre of Excellence. Prof. Gabriel Raicu is a highly regarded figure in maritime education and research, with a distinguished career at CMU spanning almost three decades. Professor Raicu has significantly enhanced the university's presence within Romania's and the European Union's research and innovation landscape, successfully coordinating a considerable number of national and EU-funded projects and making numerous contributions to conferences, academic panels and publications. Prof. Gabriel Raicu also serves as the Vice President and a founding member of the Cyber Security Cluster of Excellence (CYSCOE), a prominent Romanian cluster comprising 20 leading organisations dedicated to research and business development in cybersecurity.

Marilena Jeana CÎMPINEANU serves as director of Research, Analysis and Training Department at Euro-Atlantic Resilience Centre. She specializes in International Relations and European Studies. With almost 20 years of activity in governmental organisations, she is currently responsible with coordination of development and implementation of research projects and also of curricula development and organisation for training activities. From this position, she works to develop the research, analysis and training portofolio of the E-ARC, to identify new stakeholders in this field and to consolidate the organisation profile of a hub of expertise in resilience at national, regional and international level.