CYDEF2025 White Paper

Contributed Papers

Portugal's Cyber Defence Ecosystem: Building Resilience

Vasco Prates

Building Ecosystems: The Service Board Approach

Kaltenbach Lukas, Gabi Dreo Rodosek

Introductory Note to the Papers Submitted to CYDEF 2025

This volume comprises two papers presented at the 8th International Cyber Defence Conference (CYDEF 2025), held in December 2025. Taken together, these contributions offer a theoretically and practically informed perspective on the construction of resilient cyber defence ecosystems through the integration of education, research, industry, and public policy.

The first paper, *"Portugal's Cyber Defence Ecosystem: Building Resilience"* by Vasco Prates, examines Portugal's national cyber defence ecosystem from strategic, legal, and institutional perspectives. With particular attention to the Cyber Defence School and the Cyber Academy and Innovation Hub (CAIH), the paper elucidates how military and civilian actors, as well as national and European frameworks, can be systematically aligned. Its principal contribution lies in conceptualizing cyberspace as a whole-of-society domain, in which resilience and digital transformation are pursued through institutional integration.

The second paper, *"Building Ecosystems: The Service Board Approach"* by Lukas Kaltenbach and Gabi Dreo Rodosek, addresses persistent fragmentation within Europe's cybersecurity landscape. Drawing on empirical experience from EU initiatives, including CONCORDIA and the European Cybersecurity Competence Ecosystem, the authors advance the service board approach as a transferable model for ecosystem governance. By operationalizing collaboration through clearly defined services, the paper provides a structured mechanism for sustainable cross-sectoral cooperation.

Read in conjunction, these papers highlight the complementarity between national-level institutional architectures and overarching governance principles for cyber ecosystems. They collectively argue that effective cyber defence extends beyond technical capability, requiring coherent institutional design and ecosystem-based approaches. The insights offered here are intended to contribute to ongoing scholarly and policy debates on cyber defence, cyber resilience, and cyber innovation, with relevance extending beyond Europe to other regions, including the Indo-Pacific.

Portugal's Cyber Defence Ecosystem: Building Resilience

Vasco Prates*

Abstract

Built upon strategic guidelines, legal frameworks, and directives, the Portuguese ecosystem for education and training in Cyber Defence demonstrates suitability and feasibility tailored to a borderless domain: Cyberspace. This paper highlights the relevance and viability of the ecosystem created by identifying and interconnecting its main actors and their respective missions, among which two key actors stand out: the Cyber Defence School (Escola de Ciberdefesa Defesa – ECD) and the Cyber Academy and Innovation Hub (CAIH). While the ECD essentially provides structured training for military and civilian personnel of the Armed Forces, the CAIH fosters public-private collaboration and cooperation, both nationally and at the European level. Together they combine operational training with research, development, and capability implementation, from a whole-society perspective. This document thus outlines initiatives that strengthen the protection of citizens and, consequently, of the State, consolidating Portugal's role in NATO and the EU and highlighting its potential in strengthening security, resilience and interoperability, the guiding principles for digital transformation.

1. Introduction

The domain of cyberspace has emerged as a critical operational environment for states, businesses, and citizens. Threats in and through cyberspace—from ransomware and phishing to state-sponsored attacks—pose risks to critical and essential infrastructure, and consequently, to democratic processes and public trust. Answering these threats requires more than technical solutions: it demands cultural changes geared towards citizen awareness and preparedness.

Portugal recognizes cyberspace as a domain of national interest, where the resilience of the state, economic stability, and the integrity of democratic institutions are continually challenged. To address this context, Portugal has developed a coherent and decentralized ecosystem that integrates cyber defence (essentially military), cybersecurity, academic research, and industrial innovation, all underpinned by a strategic and legal frameworks.

This ecosystem is revealed in two fundamental strategic documents: the National Cyber Defence Strategy (ENCD)[i] and the National Strategy for a Secure Cyberspace (ENSC)[ii]. The ENCD emphasizes the military dimension of cyber operations, aligning the Armed Forces with NATO's Strategic Concept 2022, the EU Strategic Compass, and multilateral cooperation mechanisms. In turn, the ENSC extends the responsibility for cyber resilience to citizens, businesses, and public and private entities, highlighting the importance of education, awareness, and cooperation between the public and private sectors. Both strategies converge on the principle that informed citizens and qualified professionals constitute the first line of defence.

* Portuguese Cyberdefence School Director General Staff, Navy OF5, Portugal

Contextualized within this framework, the Cyber Defence School (2022) and the Cyber Academy and Innovation Hub (2023) were created.

Together, these entities can evolve into a dual system capable of filling operational gaps, promoting cyber literacy, and supporting the digital transformation process, leading to a more robust first line of defence. This document analyses the strategic frameworks, institutional roles, and opportunities generated, concluding with recommendations to strengthen governance, expand training, and improve interoperability.

2. Analysis

Portugal's national cyberspace strategy is structured around two fundamental instruments:

The National Cyber Defence Strategy (ENCD) positions cyber defence as a fundamental pillar of national security, aligned with NATO's Strategic Concept 2022 and the European Union's Strategic Compass. The Strategy emphasizes interoperability, capability development, and its integration into cyberspace operations and joint military planning. The ENCD highlights training, innovation and development, national and international cooperation, and the strengthening and development of capabilities as essential pillars. Cyber defence education and training is treated as a national security instrument and a critical factor in protecting citizens.

In turn, the National Strategy for a Secure Cyberspace (ENSC) focuses on societal resilience across six axes: building a cybersecurity structure; combating cybercrime; protecting cyberspace and infrastructure; education, awareness, and prevention; research and development; and Cooperation.

Both strategies share essential intervention axes, such as citizen education and awareness, the promotion of public-private cooperation at national and international levels, and research, development and innovation.

a. Cyber Defence School (Escola de Ciberdefesa Defesa – ECD)

Created by Decree-Law No. 19/2022[iii] and regulated by Regulatory Decree No. 2/2023[iv], the Cyber Defence School is the joint cyber defence school of the Armed Forces, integrated into the General Staff of the Armed Forces. It is one of the key structures in the National Cyber Defence Strategy (ENCD), identified as one of the pillars for the development of the Strategy, and designed to ensure the continuous evolution of the qualifications necessary for defence human resources to conduct operations in a multi-domain environment, with a special focus on cyberspace.

The ECD is therefore responsible for cyber defence training, doctrinal development, R&D cooperation, and operational training support. Its training offerings follow the NATO training model (Bi-SC 075-007), with modular pathways at the Basic, Complementary, and Specialization (Advanced) levels, covering four essential profiles: Cyber Defender, Operations, Forensics, and Developer (see Fig.1).

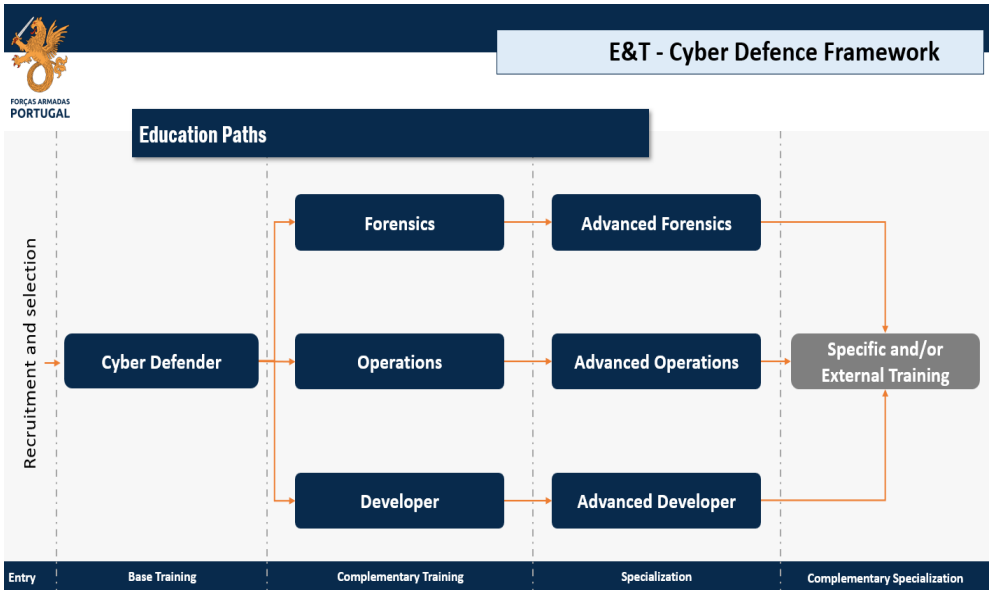

Figure 1: ECD Training Pipeline Diagram

In addition to training, ECD's responsibilities also include supporting doctrinal development and capability building; cooperating with national and international entities such as CAIH and CCDCOE; contributing to national and international exercises; and supporting research, development, and innovation.

b. Cyber Academia and Innovation Hub (CAIH) & EU-CAIH

The EU-CAIH originated in 2019 as part of a PESCO project[v] was subsequently consolidated in 2023 with Decree-Law No. 34/2023[vi] at a national level. At the national level, CAIH functions as a national association of public interest, bringing together the State, academia and industry, and as an integral component of the European project, EU-CAIH.

CAIH's mission is to enhance training, exercises, research, innovation and support for the industrial development of cyberspace. CAIH presents itself as a national and international Centre of Excellence, connecting universities, research centres, industry and public and private entities. In this context, CAIH operates in three areas: Education, Training and Exercises development (ET&D); Research, Development Innovation and Evaluation (RDI&E); and Industrial Development (ID) (see Fig. 2).

At the national level, CAIH was created as a private, non-profit association oriented towards the public interest, promoting activities in the areas of cybersecurity and cyber defence, strengthening national and European resilience and contributing to the consolidation of responses to threats in cyberspace. Its work in the areas of training and exercises is focused on developing the skills of human resources involved in cybersecurity and cyber defence.

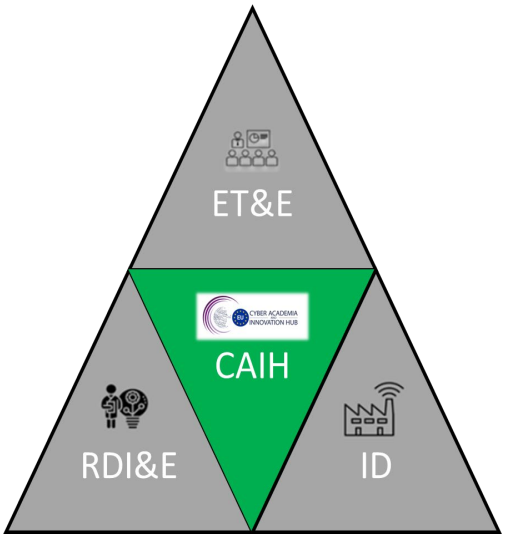

Figure 2: CAIH Orientation

c. Digital Transformation framework

Under the framework of the Strategic Directive of the General Staff of the Armed Forces (EMGFA) 2023/2026[vii], as well as by NATO's Digital Transformation Implementation Strategy [viii] and sectoral directives of the EMGFA, digital transformation embodies the continuous process of modernization, optimization and change, through which the organization implements and integrates digital technologies and solutions, generating improvements in processes, work methods, skills, changing the organizational culture and aiming at new results. In this context, four essential pillars of digital transformation are identified, namely: the Culture and Empowerment of People; the Agility of Processes; the Exploitation of Technological capabilities and innovative digital solutions; and the Efficient Management, Exploitation and Sharing of Data.

Based on essential guiding principles such as security, resilience, and interoperability (see Fig. 3), digital transformation thus encompasses concrete and fundamental lines of action and initiatives for educating and raising awareness among people, promoting public-private cooperation at national and international levels, and research, development, and innovation.

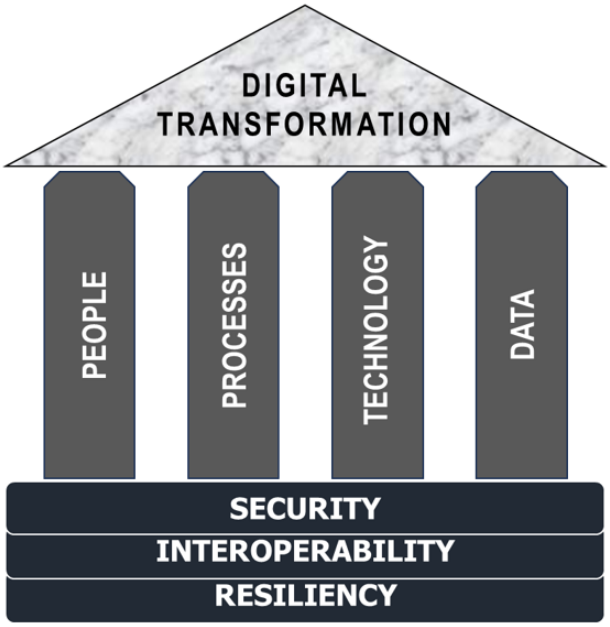

Figure 3: Digital Transformation Pillars

The digital transformation foreseen in the EMGFA directive therefore operates in several areas of interest to this article, but also in strengthening data-centric operations, integrating emerging technologies, and preparing for Multi-Domain Operations.

3. Evaluation

The Portuguese integrated model immediately presents several advantages:

- Alignment with international NATO/EU standards, promoting collaboration and cooperation initiatives resulting from the generated interoperability.
- The establishment of a formal link between defence, academia, and industry through a formal body, the CAIH.
- A focused and structured training in Cyber Defence through a formal body, the ECD.
- Consistency and alignment with actions and initiatives regarding the culture and capacity building of people and the agility of processes based on essential guiding principles such as security, resilience, and interoperability, and the digital transformation of the Armed Forces.

However, challenges persist, namely:

- The financial sustainability of private non-profit association bodies oriented towards the public interest, CAIH.
- The sustainability of a permanent body of instructors in the ECD.
- The complexity of CAIH governance; and
- Ensuring a consistent national and allied interoperability.

Education and literacy in cyberspace are not limited to the defence sector. The Portuguese dual model allows the transfer of knowledge residing in Cyber Defence to schools, public institutions, and companies, strengthening national resilience, public-private partnerships and innovation pipelines which all-in-all empower citizens to face digital threats.

4. Conclusion

Portugal presents a robust model of integrated education in cyber defence and digital transformation. Consolidating this model requires measures to mitigate the challenges and leverage the opportunities listed, where the use of Artificial Intelligence for advanced training and the intensification of international cooperation are obvious and mandatory tools.

These measures, supported by the existing strategic guidelines, legal frameworks, and directives, reinforce digital sovereignty, national resilience, and operational capacity by raising awareness and preparing citizens for the challenges and threats of cyberspace.

5. References

[i] Resolução do Conselho de Ministros n. º 106/2022 – Estratégia Nacional de Ciberdefesa (National Cyber Defence Strategy)

[ii] Resolução do Conselho de Ministros n. º 36/2015 – Estratégia Nacional de Segurança do Ciberespaço (National Strategy for a Secure Cyberspace)

[iii] Decree-Law No. 19/2022, 24th January, Organic Law of the General Staff and amends the organic laws of the three branches of the Armed Forces

[iv] Regulatory Decree n. º 2/2023, 6th of June, approves the organizational structure of the General Staff of the Armed Forces and amends the organizational structures of the Navy, Army, and Air Force.

[v] https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/ (27NOV25 15h27 WET)

[vi] Decree-Law n. º 34/2023, 23rd of May, establishes the Cyber Academy and Innovation Hub (CAIH)

[vii] Available in Portuguese language in https://www.emgfa.pt/pt/quem-somos/Documents/2023%20DEEMGFA%2023-26.pdf (27NOV25 15h28 WET)

[viiiviiiviiiviii] NATO's Digital Transformation Implementation Strategy - PO(2023) 0191 (INV), 31MAI23 and NATO's Digital Transformation Vision - PO(2022) 0405, 20SET22

Building Ecosystems: The Service Board Approach

Kaltenbach Lukas, Gabi Dreo Rodosek*

Abstract

The white paper argues that despite excellent research, committed communities, and innovative companies, Europe's cybersecurity landscape suffers from structural fragmentation. Different national priorities, federal responsibilities, separate specialist communities, and a lack of exchange formats mean that expertise is difficult to find, duplication of work occurs, and research results are slow to be put into practice. Against the backdrop of increasing digital vulnerability, growing regulatory requirements, and high innovation dynamics, neutral, resilient structures are needed that systematically connect stakeholders and make cooperation reproducible.

Building on the experiences of the H2020 pilot project CONCORDIA and the establishment of the European Cybersecurity Competence Ecosystem (ECCC, NCC, NKCS), the white paper presents the service board approach as the backbone of a European cyber ecosystem. A defined set of services (Talk, Explore, Develop, Connect, Explain, Promote, Assist, Educate) operationalizes interfaces between science, industry, administration, start-ups, and the community. In addition, specific "pacts" (in particular Research, Industry, Promotion, and Community Pacts) structure the participation of the various interest groups and translate a common target architecture into concrete offerings and opportunities for participation.

The aim of the white paper is to justify the need for such a service board and to outline a transferable design that maintains intrinsic motivation and creates added value for all stakeholders.

cybersecurity ecosystem – service board – collaboration – competence network

Introduction

Digital transformation is a constant presence in research, industry, and society. New technologies open up opportunities, but at the same time increase vulnerability and create pressure for regulatory action. Security requirements, market interests, and political cycles are all overlapping. Often without shared goals or reliable formats for exchange. This leads to duplication of effort, fragmented solutions, and a slow transfer of research results into practice.

To counter this situation, neutral, resilient structures are needed that systematically connect stakeholders, make expertise discoverable, and enable reproducible collaboration. The service board principle tested in CONCORDIA offers one approach: defined services (Talk, Explore, Develop, Connect, Explain, Promote, Assist, Educate) are used to operationalize interfaces between science, business, administration, and the community. This white paper describes how such a service hub can be set up to organize cyber innovation in a scalable and objective-oriented manner.

* Military research assistant, German Armed Forces, UniBwM Code

Motivation

An international organization or nation with strong individual elements, excellent research, engaged communities, eager companies, may suffer from structural fragmentation. On an international level, national priorities and demands in sovereignty complicate coordination. On a nation level, depending on the type of state, federal competences and decisions are distributed. On a micro level, companies pursue their own goals and business interests. They exchange little information and usually wont share expertise.

The lack of a platform prevents professional coordination, makes it difficult to find experts, and prevents research from being aligned with the interests of stakeholders.

At the same time, technological progress calls for regulations and measures against threats. Industry needs practical solutions, research needs practical use cases, and politics needs expert evaluation. These domains must be connected to avoid conflicting goals and leverage opportunities.

The Service Board approach addresses the gaps by setting goals, attempting to resolve conflicting objectives, highlighting experts, providing coordination and much more.

The objective of this white-paper is therefore to justify the necessity of a service board as the backbone of European cyber ecosystems and to outline a practicable design that maintains the intrinsic motivation of stakeholders. Research gains visibility and impact, industry receives usable results, governments benefit from reliable information for decision-making, and the ecosystem as a whole becomes more resilient.

Related Work

The following section outlines key preparatory work and initiatives that form the framework for the proposed service board approach and already demonstrate its practical implementation in some areas.

CONCORDIA

CONCORDIA was part as one of four H2020 Pilot-Projects, beside ECHO, SPARTA and CyberSec4Europe, focusing on a European cybersecurity competence network, integrated into the European ecosystem for digital sovereignty. [2] It had a runtime from four years, starting in 2019 and ended in March 2023 with a budget of approximately 16 million euros and 56 partners all over Europe, containing stakeholders from industry and research. [3] Concordia delivered multiple outcomes, grouped in the categories policy, tools, education, pilots, certification and research. The service-oriented logic of the organization is of central meaning for the ecosystem, as it provides the major benefits for participating stakeholders. [1] These four initial programs led to the establishment of the network of national coordination centres (NCC) and still lay ground for the establishment of similar innovation hubs. [2] E.g., the NKCS resulted as single point of contact for the German Federal Office for Information Security (BSI), adapting the findings from Concordia.

ECCC, NCC, NKCS

Based on the work of CONCORDIA, an European wide ecosystem was established to interconnect the European NCCCs and keep exchange up, even after CONCORDIA has finished.

The European Cybersecurity Competence Centre (ECCC) works together with the network of National Coordination Centres (NCC) and aims to sustain and increase Europe's cybersecurity competences. Every nation of the 27 European member states is represented by one NCCC. They connect each nation to the European ecosystem and serve as national point of contact for cybersecurity related matter. [3]

The Service Board

To create a benefit for all parties, the service board offers multiple services, which brings benefits to the stakeholders in various flavors. By providing this service board, participants can rely on the expertise of the ecosystem. CONCORDIA, for example, outlined the following services which are also adaptable for comparable cyber innovation hubs. [1]

Talks

The Service Board provides experts, speakers, and panelists for conferences, workshops, and other formats. It covers a broad spectrum from highly technical issues to legal and regulatory topics as well as economic and strategic perspectives. This gives industry, start-ups, and government agencies low-threshold access to curated expert knowledge, while researchers can showcase their findings and engage in dialogue with professionals from industry. This creates a shared space for discourse in which needs, insights, and expectations can be coordinated at an early stage.

Explores

Research in the field of cybersecurity is usually distributed across many teams and institutions. The Service Board consolidates these activities, highlights ongoing projects and results, and creates central access points. A "Research Pact" connects researchers and provides them with structured opportunities for collaboration. For stakeholders, this means they can use the network to find specific topics, partners, and experts.

Develops

In addition to exchange and coordination, the Service Board also supports the development of concrete solutions and prototype implementations. Through an "Industry Pact," companies can contribute real-world use cases, for example, from critical infrastructures, regulated industries, or the start-up environment. Researchers pick up on these needs and work with partners from industry, government, and the community to develop new approaches, tools, and services. This results in next-generation security solutions that are not developed in an ivory tower, but are designed from the very beginning to be applicable, compliant with regulations, and market-oriented.

Connects

To leverage synergies, the Service Board connects stakeholders beyond traditional project boundaries. Researchers with similar areas of focus are brought together in focus groups, while industry partners and start-ups are provided with structured points of contact to authorities, regulators, and community initiatives. Open communication channels, such as newsletters, topic-specific forums, regular community calls, and thematic event, ensure that relevant information does not remain isolated. This creates a resilient network that can draw on existing relationships.

Explains

New regulations, funding programs, and technological developments are difficult for many stakeholders to understand. The Service Board acts as a mediator and interpreter in this regard. Experts prepare complex technical topics in an understandable way, highlight their impact on businesses, government and society. This provides decision-makers in politics, government agencies and companies with a substantiated basis for making strategic decisions and setting priorities in a targeted manner. At the same time, researchers and start-ups are informed about regulatory developments at an early stage and can incorporate them into their planning.

Promotes

Issues with high social relevance, such as diversity, digital sovereignty, and skills retention, need visibility and support. The Service Board identifies such priorities and actively promotes them to relevant target groups, from political bodies to associations and companies to the general public. Existing networks are used to present initiatives and talent, highlight success stories, and bundle support services.

Assists

Start-ups and smaller companies in particular are often overwhelmed by complex security requirements, certifications, and compliance regulations. The Service Board offers guidance and support in this area, for example, through guidelines, checklists, best practices, and access to experts who can help select suitable standards, tools, and procedures. At the same time, policymakers and administrators also benefit. Expert groups within the network prepare topics in a structured manner, evaluate existing measures, and provide evidence-based recommendations.

Educates

Sustainable cybersecurity requires long-term skills development. The Service Board maps and connects existing educational offerings, from specialized degree programs to part-time training courses, cyber ranges, and certification programs to materials for schools. For professionals, the network offers structured learning paths, such as programs like “Becoming a Cybersecurity Consultant,” which combine technical, organizational, and regulatory aspects. At the same time, teachers and educational institutions are supported with practical resources and methodologies to anchor cybersecurity early on in education. This creates a continuous “talent pipeline” from school to university to industry, administration, and start-up ecosystems.

Objective-Oriented Ecosystem

In order for the services and pacts described above to have a real impact, the ecosystem needs well-defined goals that all five stakeholder groups, industry, research, government, community, and start-ups, can align themselves with. Without such a common goal architecture, even well-intentioned activities run the risk of running parallel to each other, fragmenting resources, and in the end only achieving isolated effects.

The organization must therefore define an ultimate mission statement (e.g., strengthening European cyber resilience) and specific, measurable goals that are comprehensible to all parties involved. These goals should be chosen in such a way that, ideally, each stakeholder group can recognize a direct benefit.

Pacts

The pacts represent the organizational interfaces between the ecosystem and various interest groups, particularly research, industry, government/authorities, community/civil society, and start-ups. They structure how these groups can interact with the Service Board and translate general goals into concrete opportunities for participation. [1]

Research Pact

Research thrives on cooperation, exchange, and visibility. The Research Pact therefore addresses individual researchers, research groups, and institutions in the field of cybersecurity. Researchers are explicitly invited to contribute ideas, project proposals, and needs to the ecosystem. The Service Board helps them find suitable partners from industry, start-ups, public authorities, or the community to turn an idea into a joint project.

Industry Pact

The industry relies on new technologies, robust security solutions, and reliable regulatory frameworks. The Industry Pact addresses companies of all sizes, from corporations and SMEs to technology-oriented start-ups. Companies are encouraged to contribute their challenges and specific use cases. Through the network, these challenges can be discussed directly with research groups, start-ups, and public authorities in order to initiate joint projects, prototypes, or pilot programs. At the same time, companies gain early insight into research and technology trends, which helps them make strategic technology decisions and investments.

Community Pact

In addition to industry and research, the state, authorities, national and international communities and civil society actors play a central role. The Community Pact is the link that integrates these actors into the ecosystem. Government agencies and public institutions contribute funding programs, political priorities and regulatory developments and, in return, receive feedback from research, industry and the community. The Community Pact thus ensures that cybersecurity is understood and addressed as a task for society as a whole and not as an isolated expert problem.

Within the Community Pact, particular groups are further specified in order to structure cooperation with governmental and non-governmental actors as well as standardization bodies.

National Cybersecurity Competence Centers and Agencies Stakeholders Group (NSG)

The NSG connects the national authorities to create a competence-network and interleave national ecosystems. They focus on awareness, policies and governance on a national level.

Observer Stakeholders Group (OSG)

Standardization and certification organizations provide boundaries and observe and coordinate the progress of the ecosystem's findings. They form the basis for creating a cybersecurity certification framework.

Liaisons Stakeholders Group (LSG)

Next to the national, there are also cross-border institutions which may be included and require coordination. allow the service board to attach at a higher level of governance and include a broader scope into the ecosystem.

Promotion Pact

An ecosystem of this kind is not only a professional network, but also a platform for visibility. The Promotion Pact addresses all stakeholders who want to make topics, offerings, or talent more visible. Courses, training programs, cyber ranges, events, tools, projects, or job openings can be specifically promoted through the network. This increases the reach and impact of existing offerings without having to establish separate, isolated communication channels for each initiative.

References

[1] Concordia, "Concordia," [Online]. Available: https://www.concordia-h2020.eu/. [Accessed 20 November 2025].

[2] European Commission, "CORDIS - EU research results," 11 June 2024. [Online]. Available: https://cordis.europa.eu/project/id/830927/reporting. [Accessed 20 November 2025].

[3] European Parliament, "EUR-Lex," 20 May 2021. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2021/887/oj/eng. [Accessed 20 November 2025].

[4] ECCC, "European Cybersecurity Competence Centre and Network," [Online]. Available: https://cybersecurity-centre.europa.eu/. [Accessed 20 November 2025].

[5] Cyberwatching, "Four EU pilot projects launched to prepare the European Cybersecurity Competence Network," [Online]. Available: https://www.cyberwatching.eu/news-events/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network. [Accessed 20 November 2025].