

D4.2 National case studies booklet on cybersecurity technology and information transfer

Work package	WP4 Know-how, good practice sharing, and information transfer activities
Task	T4.1 Best practices and case studies for enhanced cooperation between the two cybersecurity communities
Due date	30 November 2025
Submission date	12 December 2025
Deliverable lead	ULB
Version	v 3.0
Author	Jose Martinez-Usero (AMETIC)
Reviewers	Josep Bosch (AMETIC), Gabor Varga (IVSZ), Ines Vlahovic (CCIS), Balázs Tordai (IVSZ), Virgilijus Dirma (INFOBALT), Milda Savickaitė (INFOBALT) Palina Shauchuk (ULB)

Abstract

This deliverable presents a comparative analysis of cybersecurity technology transfer and information sharing frameworks across four EU Member States: Lithuania, Spain, Hungary, and Slovenia. Through a combination of desk research, stakeholder interviews, surveys, and validation workshops, the study identifies common challenges, best practices, and national divergences in cybersecurity governance, innovation ecosystems, and cross-sectoral collaboration. The findings underscore the importance of harmonised legal frameworks, institutional coordination, and investment in dual-use technologies to enhance EU-wide cybersecurity resilience.

Keywords

Cybersecurity, Technology Transfer, Information Sharing, Dual-Use Technologies, NIS 2 Directive, Innovation Ecosystems, Governance, EU Policy, CERT, ISAC, Digital Sovereignty

Document revision history

Version	Date	Description of change	Contributor(s)
VO.1	30.03.2025	Draft methodological approach and ToC	José Martínez-Usero (AMETIC), Josep Bosch (AMETIC)
VO.2	15.05.2025	Preparation of final deliverable template for national case studies	Jose Martinez-Usero (AMETIC), Josep Bosch (AMETIC), Ines Vlahovic (CCIS), Gabor Varga (IVSZ), Virgilijus Dirma (INFOBALT), Milda Savickaitė (INFOBALT)
VO.3	24.11.2025	Draft national case studies production	Jose Martinez-Usero (AMETIC), Josep Bosch (AMETIC), Albert Anglarill (AMETIC), Ines Vlahovic (CCIS), Gabor Varga (IVSZ), Balázs Tordai (IVSZ), Virgilijus Dirma (INFOBALT), Milda Savickaitė (INFOBALT)
VO.4	26.11.2025	Final national case studies available	Jose Martinez-Usero (AMETIC), Josep Bosch (AMETIC), Albert Anglarill

			(AMETIC), Ines Vlahovic (CCIS), Gabor Varga (IVSZ), Balázs Tordai (IVSZ), Virgilijus Dirma (INFOBALT), Milda Savickaitė (INFOBALT)
V1.0	02.12.2025	Draft table of contents	José Martínez-Usero (AMETIC)
V1.1	04.12.2025	Revision from coordinator	Sara Giona (28Digital)
V2.0	05.12.2025	First version of the booklet	José Martínez-Usero (AMETIC)
V2.1	05.12.2025	Revision from Hungary	Gabor Varga (IVSZ)
V2.2	08.12.2025	Revision from CCIS	Ines Vlahovic (CCIS)
V2.3	08.12.2025	Additional revision from IVSZ	Gabor Varga (IVSZ)
V2.4	09.12.2025	Revision from AMETIC	Josep Bosch (AMETIC), Albert Anglarill (AMETIC)
V2.5	10.12.2025	Revision from WP leader	Palina Shauchuk (ULB)
V3.0	11.12.2025	Revision from AMETIC	José Martínez-Usero (AMETIC)
V4.0	12.23.2025	Finaver Version	Alessandra Zini, Sara Giona (28DIGITAL)

Disclaimer

The COcyber project funded under Grant Agreement No. 101158606 is supported by the European Cybersecurity Competence Centre and funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Copyright notice

© COcyber 2024-2026

Project funded by the European Commission in the Digital Europe Programme

Nature of the deliverable	R
Dissemination level	
Public – fully open. e.g., website	✓
Sensitive (SEN) – limited under the conditions of the Grant Agreement	
EU classified — RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444	

Table of Contents

LIST OF ABBREVIATIONS AND ACRONYMS.....6

EXECUTIVE SUMMARY 7

1. INTRODUCTION8

2. METHODOLOGY9

 2.1 RESEARCH METHODS 9

3. NATIONAL CYBERSECURITY LANDSCAPE10

4. TECHNOLOGY TRANSFER FRAMEWORK 12

5. INFORMATION SHARING MECHANISMS..... 13

6. ANALYSIS OF DUAL-USE TECHNOLOGIES 15

7. RECOMMENDATIONS 16

8. CONCLUSIONS..... 18

9. ANNEXES..... 19

List of abbreviations and acronyms

Abbreviation or Acronym	Description
AMETIC	The National Digital Industry Association of Spain, COcyber partner leading the synergies with existing initiatives, exploitation and sustainability (Work Package 6), and responsible for the National Case Studies Booklet on cybersecurity technology and information transfer, and the Spanish Report (Work Package 4).
CERT	Computer Emergency Response Team, a group of information security experts who identify, analyse and mitigate cybersecurity incidents and threats.
COcyber	Coordination between the Cybersecurity Civilian and Defence Spheres. It is the project to which this booklet belongs—specifically, it is part of Task 4.1 within Work Package 4.
CSIRT	Computer Security Incident Response Team
ECCC	The European Cybersecurity Competence Centre, the funding authority of the COcyber project.
ECSF	Cybersecurity Skills Framework
ENISA	European Union Agency for Cybersecurity
EU	The European Union (EU) is a political and economic union of 27 European countries, designed to foster economic cooperation, promote peace, and create a single market with free movement of goods, services, and people.
ISACs	Information Sharing and Analysis Centres, non-profit organisations that provide a central resource for gathering information on cyberthreats.
M&E	Monitoring and Evaluation
NIS 2	Directive (EU) 2022/2555 (updated Network and Information Systems Directive).
R&D	Research and Development
SME	Small and Medium-size Enterprises
STIX/TAXII	Standardised threat intelligence formats (mentioned in the context of protocol standardisation)
TTOs	Technology Transfer Offices

Executive summary

Cybersecurity has become a cornerstone of digital sovereignty and resilience across the European Union. As cyber threats evolve in scale and sophistication, the capacity to transfer technology and share critical information across sectors and borders has emerged as a fundamental strategic priority. Deliverable 4.2 of the COcyber project presents a comparative analysis of four national case studies¹—[Lithuania](#), [Spain](#), [Hungary](#), and [Slovenia](#)—focused on cybersecurity technology, information transfer and dual use.

The COcyber project seeks to support enhanced cooperation between defence and civilian cybersecurity communities across Europe. Within this framework, Deliverable 4.2 aims to:

- Document and compare national approaches to cybersecurity technology transfer and information sharing.
- Identify systemic barriers and enabling factors in policy, legal, and institutional frameworks.
- Provide actionable insights and recommendations to strengthen cross-sectoral collaboration and innovation.

Each national case study employed a harmonised mixed-methods research design, including:

- Desk research on legal, regulatory, and policy frameworks.
- Semi-structured interviews with public authorities, industry stakeholders, defence actors, and academia.
- Online surveys capturing stakeholder perceptions and operational experiences.
- National validation workshops to refine and verify findings.

This multi-layered methodology ensured the generation of both comparable and context-sensitive insights. Some key findings are:

- National cybersecurity strategies: While all countries align with EU cybersecurity objectives, their levels of implementation maturity and stakeholder coordination differ significantly. Lithuania and Spain demonstrate advanced governance

¹ The four national case studies are available in open access on Zenodo

- AMETIC (2025). Spain case study on cybersecurity technology and information transfer.

Zenodo. <https://doi.org/10.5281/zenodo.17899220>

- Chamber of Commerce and Industry of Slovenia – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>

- INFOBALT (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>

- IVSZ – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>

structures; in Hungary cybersecurity strategy is not perceived uniformly across sectors, with the public sector assessing it more favourably; Slovenia has a strategy from 2016 that needs to be updated for today's and future developments.

- Technology transfer: Spain and Lithuania benefit from innovation clusters and supportive frameworks; Hungary and Slovenia are constrained by regulatory ambiguity and limited institutional capacity.
- Information sharing: Formal mechanisms exist in all countries, but operational trust and cross-sectoral integration remain uneven, especially in Hungary and Slovenia.
- Dual-use technologies: Definitions and regulatory frameworks vary widely. Spain and Lithuania incorporate dual-use into innovation policy, while Hungary and Slovenia require clearer structures and support.

The analysis reveals both convergence and fragmentation across the four Member States. To build a coherent European cybersecurity ecosystem, there is a need for:

- Greater legal and regulatory harmonisation at the EU level.
- Stronger national governance structures with cross-sectoral mandates.
- Investment in cybersecurity skills, trust-building mechanisms, and dual-use innovation.

Deliverable 4.2 offers a foundation for policy dialogue, institutional benchmarking, and strategic planning to foster cybersecurity resilience and technological autonomy across the EU.

1. Introduction

The acceleration of digital transformation across critical sectors in the European Union has heightened the urgency of robust cybersecurity policies, technologies, and collaboration frameworks. As cyber threats become increasingly complex and transnational, the strategic exchange of cybersecurity technologies and information between public authorities, private actors, and research institutions becomes not only desirable but essential. Effective technology transfer and information sharing are instrumental in enabling both national resilience and EU-wide security integration.

Deliverable 4.2 of the COcyber project responds to this imperative by examining the current state of cybersecurity technology and information transfer across four EU Member States²: Lithuania, Spain, Hungary, and Slovenia. It forms part of Work Package 4,

² The four national case studies are available in open access on Zenodo

- AMETIC (2025). Spain case study on cybersecurity technology and information transfer.

Zenodo. <https://doi.org/10.5281/zenodo.17899220>

- Chamber of Commerce and Industry of Slovenia – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>

which focuses on know-how exchange, good practice sharing, and cross-sectoral transfer mechanisms. The primary aim of this deliverable is to develop a comprehensive understanding of national capabilities, challenges, and institutional dynamics in these areas, thereby informing policy alignment and operational harmonization across the EU.

Specifically, this deliverable seeks to:

- Document the existing national policy and legal frameworks governing cybersecurity technology and information transfer.
- Assess institutional maturity, including the roles of public bodies, industry, academia, and the defence sector.
- Identify practical barriers and enablers to efficient technology diffusion and threat intelligence sharing.
- Highlight successful practices and innovations that could be replicated or scaled within other EU contexts.
- Propose recommendations for national and EU-level actors to enhance alignment, interoperability, and strategic coordination.

This deliverable is in fact synthesising diverse national experiences, contributing to the broader goals of the COcyber project: to support the convergence of civilian and defence cybersecurity efforts and promote European digital strategic autonomy. The findings herein are expected to be relevant not only to national policymakers and practitioners but also to EU institutions working on regulatory frameworks, funding instruments, and capacity-building initiatives in cybersecurity.

2. Methodology

The national case studies adopt a mixed-method approach combining desk research, semi-structured interviews, an online survey, and a national expert validation event. This approach ensures comprehensive evidence collection and validation across Spain, Lithuania, Slovenia, and Hungary³.

2.1 Research methods

This section outlines the methodological framework employed in the COcyber national case studies to investigate cybersecurity technology transfer and information-sharing

-
- INFOBALT (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>
 - IVSZ – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>

mechanisms within Spain, Lithuania, Slovenia, and Hungary⁴. A mixed-methods approach was adopted to ensure a comprehensive understanding of each country's cybersecurity landscape, facilitating both depth and breadth in data collection and analysis.

The research design encompasses four key components:

- Desk research: An extensive review of national cybersecurity strategies, policies, legal frameworks, and academic literature was conducted to establish a foundational understanding of each country's cybersecurity environment.
- Semi-structured interviews: Targeted interviews with key stakeholders—including representatives from government agencies, private sector entities, academic institutions, and civil society organisations—were carried out to gather in-depth qualitative insights.
- Online survey: A structured survey was disseminated to a broader group of stakeholders to collect quantitative data and validate findings from the interviews and desk research.
- National validation events: Each country hosted an interactive session with at least 15 experts to review preliminary findings, ensuring the accuracy and relevance of the data and interpretations.

This multi-faceted methodology was designed to capture a holistic view of cybersecurity practices and challenges in each nation, providing a robust basis for comparative analysis and policy recommendations.

3. National cybersecurity landscape

This section explores the national cybersecurity frameworks of Lithuania, Spain, Hungary, and Slovenia⁵, providing a comparative overview of their policy approaches, institutional

⁴ The four national case studies are available in open access on Zenodo

- AMETIC (2025). Spain case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899220>
- Chamber of Commerce and Industry of Slovenia – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>
- INFOBALT (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>
- IVSZ – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>

⁵ The four national case studies are available in open access on Zenodo

- AMETIC (2025). Spain case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899220>
- Chamber of Commerce and Industry of Slovenia – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>
- INFOBALT (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>
- IVSZ – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>

architectures, and operational capabilities. As EU Member States align with overarching directives such as NIS 2, national implementations reveal both shared goals and divergent strategies. By examining each country's cybersecurity landscape, this section identifies the degree of policy maturity, stakeholder engagement, and the institutional coherence required to enable resilient and adaptive cybersecurity ecosystems. The analysis highlights where synergies exist and where national peculiarities shape unique trajectories.

Lithuania: Exhibits strong alignment with EU norms, proactive CERT coordination, and increasing investment in R&D. A centralised governance model allows agility.

Spain: Has a mature regulatory landscape. Nevertheless, the transposition of NIS 2 is still underway, with a draft law approved in January 2025. Robust multi-stakeholder coordination and industry involvement are key strengths.

Hungary: Emphasises national sovereignty. Hungary was one of the front-runners in NIS 2 transposition and completed the legislation early, but did so through a distinct national approach, resulting in obligations that differ significantly from those in other Member States.

Slovenia: Demonstrates progress in policy updates, has implemented NIS 2 into national legislation (ZInfV-1) and published a company-focused implementation manual, but coordination between civil and defence sectors remains a challenge.

Table 1: National policy implementation status

Country	NIS2 implementation	Public-private cooperation	International engagement
Lithuania	High	High	Moderate
Spain	Moderate	Moderate	High
Hungary	High	Moderate	Low
Slovenia	Moderate	Low	Moderate

This table reveals a spectrum of readiness and strategic alignment across the four countries. Lithuania and Hungary emerge as leaders, with advanced NIS 2 implementation. Spain has strong international engagement and structured cooperation between public and private stakeholders. Lithuania's governance model facilitates public-private cooperation and cross-sectoral trust. Hungary's emphasis on national sovereignty may limit openness to international models: the legislation introduces a significantly broader model of ex-ante supervision than envisaged in the NIS2 Directive. Slovenia's weaker governance coordination impacts implementation. These differences underscore the varying degrees of institutional maturity and the need for tailored EU support mechanisms.

4. Technology transfer framework

This section investigates the legal, institutional, and operational mechanisms underpinning cybersecurity technology transfer in Lithuania, Spain, Hungary, and Slovenia⁶. Technology transfer serves as a key enabler for innovation, resilience, and cross-sector collaboration in national cybersecurity ecosystems. The analysis explores how each country facilitates or impedes technology dissemination between academia, industry, defence, and government stakeholders. It further considers the maturity of support structures such as legal frameworks, funding instruments, and innovation platforms that drive or hinder the commercialisation and scaling of cybersecurity solutions.

Lithuania: Supports tech transfer via innovation sandboxes and EU project participation. Strong academic-industry links.

Spain: Leverages digital innovation hubs and active clusters like AMETIC to facilitate tech transfer.

Hungary: Efforts are emerging, such as CyberShield, but a lack of systemic legal harmonisation persists.

Slovenia: Possesses foundational structures, but suffers from limited financial incentives and weak institutional linkages.

⁶ The four national case studies are available in open access on Zenodo

- **AMETIC** (2025). Spain case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899220>
- **Chamber of Commerce and Industry of Slovenia** – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>
- **INFOBALT** (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>
- **IVSZ** – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>

Table 2: Technology transfer support mechanisms

Country	Legal clarity	Funding tools	Innovation ecosystems
Lithuania	Moderate	High	Moderate
Spain	High	Moderate	High
Hungary	Low	Moderate	Low
Slovenia	Moderate	Low	Low

The table illustrates differing levels of institutional support for technology transfer across the four countries. Spain stands out for its robust innovation ecosystem and clear legal guidance, underpinned by digital hubs and active clusters like AMETIC. Lithuania shows a well-developed funding environment, although legal clarity remains moderate. Hungary faces dual challenges—limited innovation infrastructure and fragmented regulations—while Slovenia struggles with both funding and ecosystem development. These disparities reveal systemic gaps that must be addressed to facilitate more equitable and effective technology transfer across the EU.

5. Information sharing mechanisms

This section examines the mechanisms through which Lithuania, Spain, Hungary, and Slovenia⁷ exchange threat intelligence and other cybersecurity-relevant information. It considers the institutional arrangements, legal enablers, technical platforms, and trust dynamics that shape information flow between government agencies, private sector

⁷ The four national case studies are available in open access on Zenodo

- AMETIC (2025). Spain case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899220>
- Chamber of Commerce and Industry of Slovenia – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>
- INFOBALT (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>
- IVSZ – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>

entities, and international partners. The analysis aims to understand how information sharing is operationalised in practice, what barriers exist, and which models hold promise for replication or scaling across the EU.

Lithuania: Operates a structured CERT model with EU integration. Encourages data sharing through public–private agreements.

Spain: Excels in platform–driven intelligence exchange and international cooperation.

Hungary: Information sharing is progressing within public administration and state–controlled enterprises, but remains hindered by mistrust beyond this circle.

Slovenia: Operating a structured CERT model with SI–CERT in a central role and developing ISACs and cross–sector bridges. However, it still lacks a centralised intelligence hub; this is only in the initial phase of development as a standalone entity.

Table 3: Threat intelligence sharing maturity

Country	CERT/CSIRT centralisation	Platform utilisation	Cross–sectoral trust
Lithuania	High	Moderate	Moderate
Spain	High	High	Moderate
Hungary	High	Low	Low
Slovenia	Moderate	Moderate	Low

The data presented highlights a varied landscape in terms of threat intelligence sharing capabilities. Lithuania, Spain and Hungary demonstrate high levels of CERT/CSIRT centralisation, which enables coordinated and timely responses to cyber threats. Spain’s advanced use of sharing platforms further positions it as a regional leader in operational threat intelligence. In contrast, Hungary’s fragmented and trust–deficient environment inhibits sharing effectiveness. Slovenia, while developing relevant structures, remains limited by insufficient exchange with the industry. This heterogeneity underscores the

importance of fostering trust, standardising protocols, and investing in interoperable platforms to support efficient and secure information exchange across Member States.

6. Analysis of dual-use technologies

This section explores the concept and implementation of dual-use cybersecurity technologies—solutions that serve both civilian and defence applications. Dual-use innovation is increasingly vital as national security and economic competitiveness become interlinked in the digital era. The analysis focuses on how Lithuania, Spain, Hungary, and Slovenia⁸ define, regulate, and promote dual-use technologies within their cybersecurity strategies. It evaluates the legal frameworks, innovation incentives, export control mechanisms, and real-world applications that shape the trajectory of dual-use development in each country.

Lithuania: Promotes dual-use development through public innovation grants and European partnerships.

Spain: Integrates dual-use into broader industrial and defence innovation policies.

Hungary: Treats dual-use primarily through a defence lens, with limited civilian spinoff.

Slovenia: Highlights dual-use potential but lacks operational frameworks for support.

Table 4: National support for dual-use cybersecurity R&D

Country	Definition clarity	Innovation support	Export controls
Lithuania	High	High	Moderate
Spain	High	Moderate	High

⁸ The four national case studies are available in open access on Zenodo

- AMETIC (2025). Spain case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899220>
- Chamber of Commerce and Industry of Slovenia – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>
- INFOBALT (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>
- IVSZ – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>

Hungary	Low	Low	High
Slovenia	Moderate	Moderate	High

The table presents notable variation in how each country approaches dual-use technology governance and support. Lithuania and Spain lead with clear definitions and strong innovation backing, supported by grants and integration into national strategies. Spain also demonstrates comprehensive export control procedures, which balance innovation with security. Hungary’s dual-use ecosystem remains underdeveloped, and civilian R&D is frequently oriented towards export markets rather than strengthening domestic capabilities. Slovenia, while recognising the potential of dual-use, lacks operational support structures. These discrepancies highlight the urgent need for a harmonised EU-wide approach to dual-use technology that aligns innovation, compliance, and strategic autonomy.

7. Recommendations

This section consolidates the comparative findings derived from the four national case studies and articulates a series of evidence-based policy recommendations. These recommendations aim to address both the systemic challenges and the strategic opportunities identified across Lithuania, Spain, Hungary, and Slovenia⁹. By leveraging the diversity of national experiences, the proposed actions seek to advance a more integrated, resilient, and innovation-driven European cybersecurity landscape. The recommendations are structured thematically to guide decision-makers at both national and EU levels in strengthening governance, legal coherence, institutional capacity, and technological innovation.

Governance structures: Member States should institutionalise cross-sectoral governance bodies that include representatives from government, defence, industry, and academia. These bodies should be endowed with decision-making authority and tasked with the strategic alignment of national cybersecurity objectives, ensuring coherence

⁹ The four national case studies are available in open access on Zenodo

- AMETIC (2025). Spain case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899220>
- Chamber of Commerce and Industry of Slovenia – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>
- INFOBALT (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>
- IVSZ – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>

between civilian and military domains. Such governance frameworks must be integrated with EU-level structures to enhance interoperability and policy coherence across Member States.

Legal and regulatory harmonisation: There is a critical need to harmonise legal definitions and operational frameworks related to cybersecurity technology transfer and dual-use technologies. Diverging national interpretations hinder collaboration and technology mobility. The European Commission should consider issuing guidelines, promoting best practices or soft law instruments to promote consistent regulatory practices, while national legislatures should adapt their statutes to reduce legal fragmentation and regulatory uncertainty in order to reduce the time from project idea to commercialisation.

Capacity building and skills development: Investments in human capital are foundational to cybersecurity resilience. Member States should adopt national strategies for cybersecurity education and workforce development, incorporating standardised training modules, certifications aligned with the European Cybersecurity Skills Framework (ECSF), and cross-sectoral simulation exercises. Joint training between civilian and military personnel can foster mutual understanding and operational synergy.

Information sharing ecosystems: To foster trust-based information sharing, Member States should institutionalise national Information Sharing and Analysis Centres (ISACs) with cross-sectoral mandates. These ISACs should operate alongside CERTs/CSIRTs and be supported by legal guarantees of confidentiality and data protection. EU-level support should include funding for platform development and the establishment of protocols for standardised threat intelligence formats, such as STIX/TAXII.

Innovation and technology transfer mechanisms: Member States should strengthen national innovation ecosystems through targeted R&D incentives, public procurement programs that prioritise cybersecurity solutions, and technology transfer offices (TTOs) embedded within universities and research centres. Particular attention should be given to facilitating the commercialisation of research outputs and fostering SME participation in cybersecurity innovation.

Support for dual-use technology development: Given the strategic relevance of dual-use technologies, Member States should implement clear, innovation-friendly frameworks that address the licensing, export control, standards, and compliance challenges inherent to dual-use solutions. This includes defining criteria for dual-use classification, providing legal guidance for developers, and integrating dual-use considerations into national innovation strategies. Collaboration with EU agencies such as ENISA and the European Defence Fund can amplify impact.

Strategic funding and coordination: The European Union should continue to offer dedicated funding instruments under the Digital Europe Programme, EDA, EDF and Horizon Europe to support cybersecurity R&D, especially for projects with cross-border or dual-use potential. Coordination mechanisms should ensure that national investments align with EU priorities and avoid duplication while maximising synergies among Member States.

Monitoring, evaluation, and policy learning: All cybersecurity initiatives, particularly those involving information sharing and technology transfer, should include robust monitoring and evaluation (M&E) frameworks. These should combine qualitative and quantitative metrics and feed into continuous policy learning processes at both national and EU levels. Periodic peer reviews and benchmarking exercises can support knowledge diffusion and best practice replication including the dissemination of information on project results.

8. Conclusions

This concluding section draws together the key insights from each thematic chapter, offering a consolidated overview of the comparative findings from the four national case studies. While significant divergences exist in legal, institutional, and operational frameworks across Lithuania, Spain, Hungary, and Slovenia¹⁰, the synthesis also reveals common patterns and shared challenges. Each specific conclusion below corresponds to a chapter of this deliverable and presents a targeted conclusion reflecting on the core lessons and implications for EU-wide cybersecurity development.

The national cybersecurity landscapes exhibit varying levels of maturity, with Lithuania and Spain showing advanced strategic alignment and stakeholder integration. Hungary has set out ambitious policies, yet there is uncertainty over their implementation in practice. Slovenia faces challenges in governance coordination and strategy implementation. Strategic harmonisation and enhanced institutional alignment are essential to bridging these gaps across the EU.

Technology transfer remains a fragmented and under-optimised process in most Member States. Spain and Lithuania provide promising models through innovation clusters and

¹⁰ The four national case studies are available in open access on Zenodo

- AMETIC (2025). Spain case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899220>
- Chamber of Commerce and Industry of Slovenia – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>
- INFOBALT (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>
- IVSZ – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>

legal facilitation, while Hungary and Slovenia must enhance their institutional capacity and funding tools. EU guidance on best practices and innovation governance could accelerate convergence.

All four countries operate formal sharing structures, yet the degree of cross-sectoral integration and platform utilisation varies considerably. Lithuania and Spain are more advanced, whereas Hungary and Slovenia need greater investment in trust-building and operational interoperability. EU-wide standardisation and secure sharing frameworks are necessary.

The governance of dual-use technologies is inconsistent across the case studies, with Lithuania and Spain demonstrating forward-thinking strategies, Hungary requiring clearer definitions and support frameworks, and Slovenia requiring more incentives and the removal of obstacles to cooperation between research and development and exploitation in operational use. A harmonised EU policy on dual-use cybersecurity innovation would help unify approaches and reduce regulatory burdens.

The comparative evidence suggests that national progress in cybersecurity technology and information transfer is uneven but can be improved through coordinated action. Member States must invest in institutional development, legal harmonisation, R&D incentives, and strategic capacity building to create a secure and resilient European cybersecurity landscape.

The integration of cybersecurity technology and information transfer frameworks across Member States remains uneven. While Lithuania and Spain demonstrate institutional maturity and multistakeholder engagement, Hungary's cyber resilience would be strengthened by higher levels of trust across the ecosystem, including both cross-sectoral and cross-border cooperation. Slovenia needs a stronger institutional solution which will facilitate innovation and coordinate all efforts in technology and information transfer (including dual use).

9. Annexes

AMETIC. (2025). Spain case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899220>

Chamber of Commerce and Industry of Slovenia – CCIS. (2025). Slovenian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17899007>

INFOBALT. (2025). Lithuanian case study on cybersecurity technology and information transfer. Zenodo. <https://doi.org/10.5281/zenodo.17898946>

IVSZ – Hungarian Association of Digital Companies. (2025). National case study on cybersecurity technology and information transfer – HUNGARY. Zenodo. <https://doi.org/10.5281/zenodo.17898415>