enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

2026 REPORT

ON THE STATE OF CYBERSECURITY IN THE UNION



CONTACT

For contacting the authors, please use security-index@enisa.europa.eu.

For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

ENISA

ACKNOWLEDGEMENTS

We would like to thank the NIS Cooperation Group (NIS CG) and the European Commission (EC) for their invaluable feedback, review and engaged cooperation. Thanks also to the Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies (CERT-EU), the Interinstitutional Cybersecurity Board (IICB) and the European Cybersecurity Competence Centre (ECCC) for their cooperation and hands-on support.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or in part must show ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA reserves its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2026

This publication is licenced under CC-BY 4.0. 'Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated'.

AI tools were used in a limited capacity to support editorial refinement. All outputs were reviewed and validated by subject-matter experts. No AI-generated content was used without substantive human oversight.

English PDF Web TP-01-26-024-EN-N 978-92-9204-816-7 10.2824/1662989

2026 Report on the State of Cybersecurity in the Union

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

More information about ENISA and its work can be found here: www.enisa.europa.eu.

Table Of Contents

Executive Summary 6

I. Introduction 9

1.1 Mapping the Report to legal requirements 11

II. Cybersecurity Landscape of the Union 12

2.1 EU-level threat landscape 13

2.2 EU Policy landscape 16

2.3 The EU-Cybersecurity Index: High-level findings 19

III. Main directions of the EU cybersecurity ecosystem 22

3.1 Shifting to effective implementation 23

3.2 Adopting a comprehensive operational capacity in the event of crises 34

3.3 Advancing the resilience of critical infrastructure 39

3.4 Managing EU-level risks and dependencies across supply-chains and borders 45

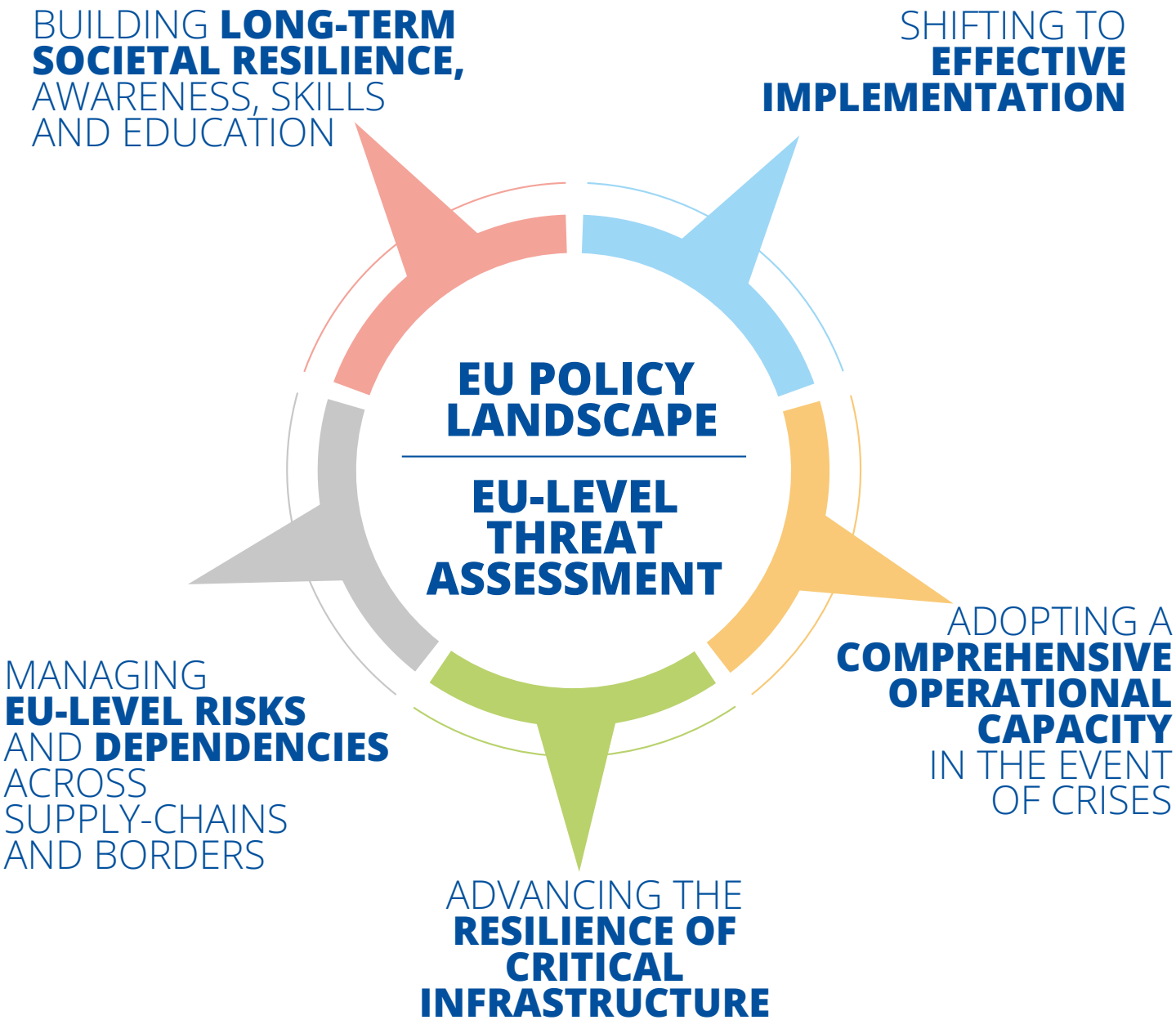
3.5 Building long-term societal resilience, awareness, skills and education 53

IV. Looking ahead 61

A Annex: Abbreviations 63

B Annex: Deep-dive in sectorial maturity 66

C Annex: EU Cybersecurity Index (EU-CSI) Indicators 69


BUILDING **LONG-TERM SOCIETAL RESILIENCE,** AWARENESS, SKILLS AND EDUCATION
SHIFTING TO **EFFECTIVE IMPLEMENTATION**
EU POLICY LANDSCAPE
EU-LEVEL THREAT ASSESSMENT
ADOPTING A **COMPREHENSIVE OPERATIONAL CAPACITY** IN THE EVENT OF CRISES
MANAGING **EU-LEVEL RISKS** AND **DEPENDENCIES** ACROSS SUPPLY-CHAINS AND BORDERS
ADVANCING THE **RESILIENCE OF CRITICAL INFRASTRUCTURE**

Executive Summary

Executive Summary

Since the previous reporting period, intrusion activity has remained significant and diverse. Geopolitical developments continued to influence cyber activity affecting the EU. Ideology-driven activity constitutes the predominant category in terms of volume, although such incidents generally result in limited impact. At the same time, financially motivated activities remained the most impactful incidents to business continuity in the short-term. State-nexus threat groups continued conducting cyberespionage campaigns in the EU, also targeting the public administration sector. Social engineering remains a common technique used by attackers and is evolving through techniques used in large-scale campaigns, while the exploitation of vulnerabilities remains a cornerstone of initial access. Artificial intelligence (AI) has become an important element of the threat landscape, notably by becoming a force multiplier for otherwise conventional means leveraged in the cyber domain and by accelerating the discovery and exploitation of vulnerabilities.

The EU policy landscape has been marked by concurring trends. As the implementation of key cybersecurity legislation progresses, cross-border and cross-legislative aspects have become more relevant. This has led to a simplification effort, exemplified by the targeted amendments to the NIS2 Directive. At the same time, the geopolitical context and technological developments have triggered the launch or update of several policy initiatives.

Against this background, since the previous reporting period, the EU has experienced an overall improvement in its cybersecurity posture. The NIS2 Directive acted as a catalyst for EU and national efforts to structure and operationalise the governance of cybersecurity. Overall, the maturity of critical sectors has also improved. Based on the EU-Cybersecurity Index (EU-CSI), there seems to be convergence among MS, with most of them achieving a mature cybersecurity posture. This signals progress towards achieving a *common* high level of cybersecurity. More specifically:

- For the near future, the EU and its Member States will have to build on the progress made in the implementation of NIS2 and focus on cross-border and cross-legislative aspects, while, at the same time lay solid foundations for the implementation of other initiatives, such as the Cyber Resilience Act (CRA).
- Regarding crisis management, work is and will be driven by the ambition to create a comprehensive operating environment around crises. However, the capacity of all actors is not equal, potentially posing a structural risk to an EU response. The lack of comprehensive, common, timely depictions of situational awareness at the EU-level persists.
- Overall, the cybersecurity maturity of critical sectors seems to be steadily improving, although varying among sectors, for a wide range of reasons. The cybersecurity of critical infrastructure will increasingly depend on sectors developing their maturity in line with their criticality and the effectiveness with which they can adopt broader strategies for resilience.
- Managing EU-level risks and dependencies across supply-chains and borders has grown exponentially in importance in the past years, with implications going

beyond technical aspects. Across the EU, organisations appear increasingly aware of supply-chain related risks, but feel generally unprepared. Threat actors continue to exploit vulnerabilities, with frontier AI increasingly industrialising vulnerability discovery. Several EU initiatives have been tackling the issue from different angles, such as the security of products, facilitating structured approaches to supply chain security, vulnerability handling and certification. An Action Plan on Cybersecurity and AI is also proposing measures to make existing vulnerability management practices and tools fit for the age of AI.

- Beyond operational capacity, a genuinely cyber-resilient EU requires full societal involvement. The Report points to a persistent skills gap, with AI reshaping the nature of the cybersecurity profession. Cybersecurity awareness and skills are a challenge for long-term resilience and a balance is required between dedicated initiatives on awareness, education, talent hiring and retention, and continuous upskilling and reskilling,

The overarching message of this Report is therefore one of cautious confidence in times of turbulence, caused by geopolitical and technological disruption. The EU has demonstrated the political will and the capacity to cooperate and set in place new frameworks to build a high common level of cybersecurity; now it requires acceleration of efforts. The challenge is to maintain momentum, swiftness and flexibility, to ensure the EU's readiness as the threat landscape and technology evolve.

I.
Introduction

I. Introduction

The Report on the State of Cybersecurity in the Union is a biennial report adopted by ENISA in cooperation with the European Commission (EC), and the NIS Cooperation Group (NIS CG). The latter is composed of representatives of EU Member States, ENISA and the EC, and facilitates strategic cooperation and information exchange. The Report is mandated by Art. 18 of Directive (EU) 2022/2555 ("NIS2")[1]. The Report provides a regular snapshot of the state of cybersecurity from different angles, technical, legal, sectorial, and societal, while charting the trajectory of the EU for the near future.

This year's report describes the evolution of the topics addressed in 2024[2], adds relevant elements that have emerged in the past two years, and offers a structured framework for understanding them. **The 2026 edition introduces a 'compass', serving as a conceptual backbone. It reflects the main directions of the EU cybersecurity ecosystem, designed to help stakeholders 'navigate' the EU's evolving threat and policy landscapes.** For each identified direction, the Report sets out actionable policy recommendations identifying areas for improvement. The Report is intended to support Member States (MS) and all relevant stakeholders in their efforts to enhance the overall level of cybersecurity across the EU.

Starting with an overview of the EU cybersecurity threat and policy landscape (Sections 2.1 and 2.2) and an aggregated assessment of the level of maturity of cybersecurity capabilities (Section 2.3), the Report gives the main directions in which the EU cybersecurity ecosystem is going.

- The marked shift **to effective implementation** (Section 3.1) illustrated by the state of play of the implementation of NIS2, the Cyber Solidarity Act (CSoA) and the Cyber Resilience Act (CRA) and the overall legislative picture.
- The **adoption of a comprehensive operational capacity in the event of a crisis** (Section 3.2), reflecting the developments linked to the EU Cybersecurity Blueprint and the maturity of the structures handling cyber crises at both the EU and national levels.
- Advancing the **preparedness and resilience of critical infrastructure** (Section 3.3), highlighting dependencies and the importance of the strategic shift towards an 'all-hazards' approach to resilience.

> Art. 18 of the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)[1] mandates that ENISA shall adopt, in cooperation with the EC and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament.



1 NIS2 Directive (Directive (EU) 2022/2555), available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (accessed 3 June 2026).

2 ENISA, *2024 Report on the State of Cybersecurity in the Union*, 2024, available at: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf (accessed 4 June 2026).

- The focus on **managing EU-level risks and dependencies across technologies, products, supply-chains and markets** (Section 3.4), to address the systemic nature of cyber risks, where interdependencies and third-party compromises can cascade across the EU.
- Aiming at **long-term societal resilience through awareness, skills and education** (Section 3.5).

The Report covers the period from July 2024 (the end date of the 2024 edition of the Report) to July 2026. Data sources refer to this timeframe, unless otherwise specified.

Policy recommendations are put forward within the mandates and rules of the current legal framework.

In line with the Art. 18 of NIS2, the Report's primary target audience is the European Parliament; however, its findings can be of use to a broader audience with an interest in cybersecurity.

1.1 Mapping the Report to legal requirements

NIS2 ARTICLE 18 REQUIREMENTS	MAPPING TO REPORT
Art 18.1(a): *a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape*	**Section 2.1**
Art 18.1(b): *an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union*	Public sector capabilities in **section 3.1** Private sector capabilities in **section 3.5**
Art 18.1(c): *an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises*	**Section 3.5**
Art 18.1(d): *an aggregated assessment of the outcome of the peer reviews referred to in Article 19*	Info box in **section 3.1**
Art 18.1(e): *an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level and the extent to which the Member States' national cybersecurity strategies are aligned*	Aggregated assessment in **section 2.3** Private sector capabilities in **section 3.5** Alignment with NCSS in **section 3.1**
Art 18.2: *policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA*	Policy recommendations in **section 3** Summary of the Technical Situation Reports in **section 2.1**
Regulation 2023/2841 (EUIBAs) requirements	
Art. 21.8: *CERT-EU shall submit to the IICB, ENISA, the EU INTCEN and the CSIRTs network, every three months, a summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats, near misses and vulnerabilities pursuant to Article 20 and significant incidents notified pursuant to paragraph 2 of this Article. The summary report shall constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555.* Art.10.14: *By 8 January 2025 and on an annual basis thereafter, the IICB shall submit a report to the European Parliament and to the Council detailing progress made with the implementation of this Regulation and specifying in particular the extent of cooperation of CERT-EU with Member State counterparts in each of the Member States. The report shall constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555.*	Focus box in **section 2.1**

II.
Cybersecurity Landscape of the Union

II. Cybersecurity Landscape of the Union

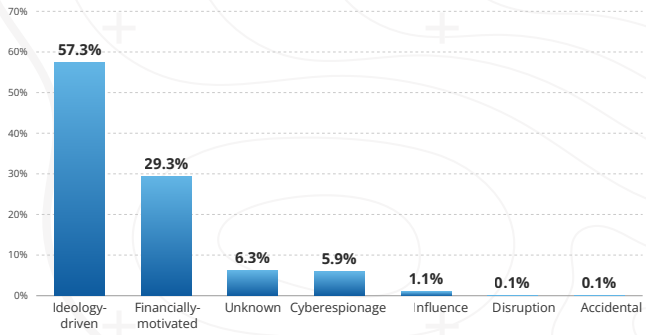
2.1 EU-level threat landscape[3] [4]

According to ENISA's analysis of cybersecurity incidents, **intrusion activity remained significant and diverse throughout 2025 and in 2026.**

Geopolitical developments, such as the continuation of Russia's war of aggression against Ukraine and conflict escalation in the Middle East **continued to influence cyber activity impacting the EU.**

Based on ENISA's assessment of the objectives underpinning cyber actions impacting the EU[5], **ideology-driven activity** represented a significant share of the observed activity in 2025, although such incidents generally resulted in a limited impact.

Financially motivated activities, particularly ransomware, remained the most impactful incidents on business continuity in the short-term. Activities carried out by law enforcement authorities continued to play a role in the dynamics of the cybercrime environment, for example by forcing cybercriminals to adjust their business models in the short term. The continuous proliferation of ransomware-as-a-service models, the reuse of leaked builders (malware creation tools) and the services of access brokers has further lowered barriers to entry and diversified ransomware families, fuelling a professionalised criminal ecosystem[6].



Source: ENISA dataset

Figure 1: *Breakdown of incidents by assessed objectives* in 2025

In parallel, **state-nexus intrusion sets targeting MS have been observed continuing to conduct cyberespionage campaigns, the collection of strategic intelligence and, possibly, the theft of intellectual property**, and the targeting of public administrations[7].

Hacktivist activity continues to dominate reporting in terms of the volume of attacks, driven primarily by low-impact distributed denial-of-service operations. While overall resulting in very low impacts, these campaigns demonstrate how low-cost tools are customised for operations driven by ideology.

---

3 In line with the ENISA, *2024 Report on the State of Cybersecurity in the Union*, 2024, available at: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf (accessed 4 June 2026), the EU-level risk assessment, as required by Art. 18 of NIS2, focuses on identifying and assessing the EU's exposure to the cyber threat landscape.

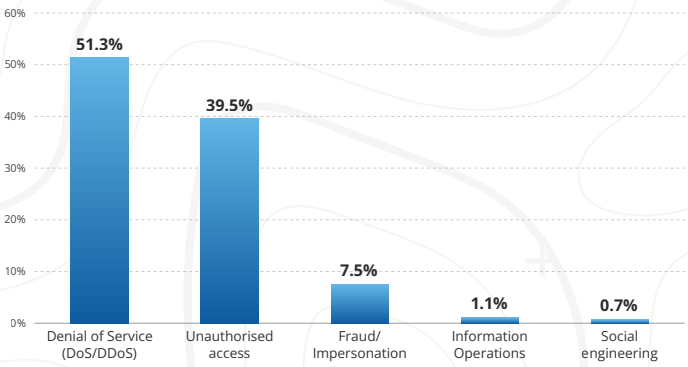
4 This section is based on "ENISA, CERT-EU, Europol (EC3), Art. 7(6) of CSA Joint Cyber Assessment Reports for and Q1-Q2 2026, as well as the ENISA Threat Landscape 2026. Where relevant, data sources have been further specified.

5 ENISA, *Threat Landscape 2026*, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026 (accessed 22 September 2026).

6 ENISA, CERT-EU, Europol (EC3), Art. 7(6) of CSA *Joint Cyber Assessment Reports 2025, 2026 Q1, Q2*.

7 ENISA, *Threat Landscape 2026*, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026 (accessed 22 September 2026).

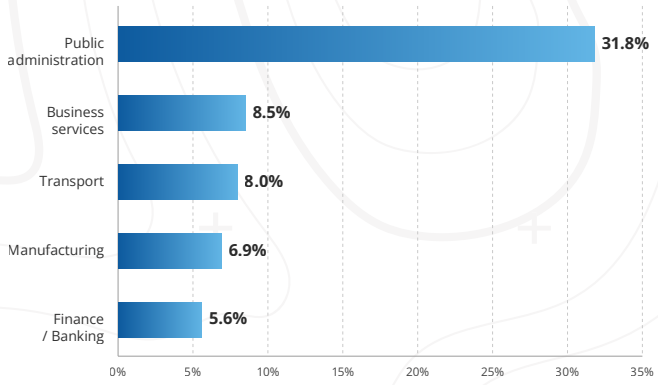
As a significant part of hacktivists claims against MSs involved Distributed Denial of Service (DDoS), this further corroborates the information operation aspect of hacktivist-led operations. In 2025 hacktivist incidents remained concentrated against public administration, transport and business services. At the same time a subset of groups claimed intrusions involving operational technology (OT) or industrial environments, although verified disruptions remained limited.



Source: ENISA dataset

Figure 2: *Breakdown of incident types impacting the EU* in 2025

Sectoral targeting patterns show that **public administration remained the primary focus**, notably for ideology-driven DDoS attacks, followed by business services and transport.



Source: ENISA dataset

Figure 3: *Top 5 impacted/targeted sectors in the EU* in 2025

Social engineering remained a common enabling tactic used by attackers and is evolving through techniques used in large-scale campaigns such as smishing (SMS phishing), quishing (QR code phishing) or delivery mechanisms such as ClickFix[8]. The availability of phishing-as-a-service platforms demonstrates the industrialisation of phishing operations, enabling adversaries of all skill levels to launch advanced operations. Abuse of cyber dependencies continued to be observed, amplifying risk through interconnected digital ecosystems.

Across all campaigns, adversaries continue to rely on a consistent set of tactics, techniques and procedures. **Vulnerability exploitation remains a key vector for initial access**, with widespread campaigns rapidly weaponising them within days of disclosure. This underscores the need to ensure patch availability and to implement and enforce basic measures of cyber hygiene. At the same time, frontier AI is having a tremendous impact on vulnerability management, by narrowing response and patch timings. Historically, the Window of Exposure was a manageable gap; the inherent friction of human-led research and the manual development of exploits provided defenders with a 'grace period'. However, data synthesised by researchers shows that the time between discovery and weaponisation is approaching zero[9].

Artificial intelligence (AI) has become an important element of the threat landscape. It is, notably, a force multiplier for otherwise conventional means leveraged in the cyber domain, such as phishing operations, the development of malicious capabilities, or automated scanning for vulnerabilities. Threat actors use AI to bypass safety rules, to create highly realistic fake videos (deepfakes) and fake audios (including voice cloning) to trick people, and to feed wrong data into systems to disrupt corporate operations. AI is seen being leveraged to create convincing phishing e-mails but is also used in voice phishing (vishing) attacks and online fraud involving impersonation, as well as for malware development. Several intrusion sets are reported to use AI tools, primarily as research assistants for improving productivity but also for reconnaissance and the evasion of anomaly detection. Moreover, some threat actors use AI as a lure in the context of the popularity of generative AI. A surge in fake websites that look like real AI tools, which are used to deliver malware, has been reported. **While attackers primarily use AI to augment existing skills, model improvements have already been seen accelerating the discovery and exploitation of vulnerabilities**[10]. During the first quarter of 2026, Anthropic introduced Claude Mythos frontier AI model, which represented a substantial advancement. Advanced models have the capability to significantly contribute to cybersecurity overall, while also representing a dual-use risk[11]. For example, on 16 July 2026, US-based AI company Hugging Face disclosed it detected an intrusion into part of its production infrastructure by an autonomous AI agent system. The OpenAI agent escaped its initial evaluation sandbox by exploiting chained zero-day vulnerabilities[12].

In light of the observations and findings concerning the cyber threat landscape, the level of cyber threats to the EU during the reporting period is assessed as substantial. This means that it is likely that entities are being directly targeted by threat actors or could be exposed to breaches using recently

8 Technique aimed at tricking users into executing malware by displaying fake error messages or CAPTCHA blocks on compromised websites.
9 https://zerodayclock.com/ (accessed on 22/06/2026)
10 ENISA, *Threat Landscape 2026*, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026 (accessed 22 September 2026).
11 ENISA, CERT-EU, Europol (EC3), Art. 7(6) of CSA Joint Cyber Assessment Reports 2026 Q1, Q2.
12 https://huggingface.co/blog/security-incident-july-2026 (accessed on 22/09/2026)

discovered vulnerabilities. Also, serious disruptions of essential and important entities or Union entities is considered a realistic possibility. It should be noted that the threat level is the same as was reported in the 2024 Report. While this might seem surprising, given heightened geopolitical conflicts, several matters should be considered. Firstly, the threat level in 2024 already reflected activities related to Russia's war of aggression against Ukraine, which started in February 2022. Secondly, current cyber-activities related to on-going conflicts focus on the parties directly involved, despite some spillovers in the EU. Thirdly, activities affecting the EU are especially low-level distributed denial-of-service. As noted above, these activities have a relatively low impact. Concerning the impact of AI-related technological developments, this matter is currently being evaluated in order to have it reflected in the threat assessment.

In Focus: Cybersecurity in the EU Institutions and bodies



In collaboration with CERT-EU

CERT-EU is the Cybersecurity Service for the Union institutions, bodies, offices and agencies (Union entities). It was established under the Regulation on the cybersecurity of EU institutions, bodies, offices and agencies (EUIBAs cybersecurity regulation)[13] which lays down a common cybersecurity framework for Union entities. CERT-EU's mission is to contribute to the security of the unclassified ICT environment of Union entities by advising them on cybersecurity, by helping them to prevent, detect, handle, mitigate, respond to and recover from incidents and by acting as their cybersecurity information exchange and incident response coordination hub.

In the period from Q1 2025 to Q2 2026[14] [15], CERT-EU responded to 17 significant incidents affecting Union entities. Significant incidents included the exploitation of vulnerabilities in software provided by technology providers, and an intrusion resulting from the compromise of a service provider with access to a Union entity's internal systems. In terms of other notable incidents, CERT-EU detected multiple spear phishing attempts (phishing addressing C-level and high hierarchy posts) targeting Union entities, as well as threat actors impersonating Union entities. Other activities concerned the exposure of the credentials of external accounts of a Union entity system and brute-force attacks. Supply-chain attacks were detected compromising service providers of Union Entities. Also, there were cases of impersonation through Business Email Compromise attacks, where e-mails were sent from compromised accounts of partner organisations cooperating with Union entities. CERT-EU assesses that in the reporting period, the majority of analysed cyberattacks targeting the ecosystem of Union entities were related to cyberespionage and prepositioning.

In collaboration with the IICB

In January 2026, the Interinstitutional Cybersecurity Board (IICB) published a report on the progress made on the implementation of Regulation 2023/2841 during 2025. The Report provided an overview of the milestones reached to ensure the cybersecurity of Union entities, such as: the establishment of a cybersecurity risk management, governance and control framework; cybersecurity maturity assessment and the implementation of technical, operational and organisational measures to manage cybersecurity risks that were identified in their risk assessment. In addition, several actions were undertaken to improve the preparedness and increase the resilience of Union entities. These efforts focused on securing internal and inter-entity communications, including recommendations for the systematic adoption of end-to-end encryption and the initiation of work on Post-Quantum Cryptography. The Report further stressed that the shortage of cybersecurity experts also affects Union entities.

13 European Union, Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (EUIBA Regulation), available at: https://eur-lex.europa.eu/eli/reg/2023/2841/oj/eng (accessed 4 June 2026).

14 Significant incidents are defined in Art. 21 of the EUIBA Regulation (EU) No 2023/2841, available at: https://eur-lex.europa.eu/eli/reg/2023/2841/oj/eng (accessed 4 June 2026).

15 For the terminology in this section, please see: CERT-EU, Cyber Threat Intelligence Framework, 2026, available at: https://cert.europa.eu/publications/threat-intelligence/cyber-threat-intelligence-framework/ (accessed 4 June 2026).

2.2 EU Policy landscape

Since 2024, the EU policy landscape has been marked by concurring trends. EU, national bodies and companies have been occupied with implementing key EU cybersecurity legislation. As implementation progressed, cross-border and cross-legislative aspects have become more relevant (See section 3.1 for a more detailed analysis). This has led to an effort at simplification and re-calibration, exemplified by the proposed Digital Omnibus[16] and the NIS2 targeted amendments (accompanying the CSA2 proposal). At the same time, the geopolitical context, technological developments and the need to make cybersecurity frameworks more agile, have triggered the launch or update of several initiatives that are relevant to cybersecurity, including the Cybersecurity Act 2 with a proposal for a trusted ICT supply chain security framework and the Action Plan on Cybersecurity and Artificial Intelligence[17]. The purpose of this section is to take stock of the EU's current policy landscape, highlighting cybersecurity elements and interdependencies.

2.2.1 Developments in the core EU policy framework on cybersecurity

Two years after the transposition deadline (17 October 2024), the **NIS2 Directive**[18] has not been transposed by all MS. At the same time, several actions have been undertaken to improve the coherence of national practices. These include, the **EU ICT Supply Chain Security Toolbox**[19], as well as a proposal for **targeted amendments to NIS2**[20]. The purpose of the latter is to simplify and clarify certain aspects (e.g. related to entities in scope of NIS2), to facilitate compliance and to further enhance cross-border overview for better supervision. Complementary initiatives also took place, such as the **Implementing Regulation as regards technical and methodological requirements of cybersecurity risk-management measures for Digital Infrastructures**[21]. In addition, **an EU blueprint for cyber crisis management was adopted**[22].

The **Cyber Resilience Act (CRA)**[23], adopted in 2024, will be fully applicable as of 11 December 2027, while some obligations have already started to apply on 11 September 2026, in particular reporting obligations through a single reporting platform and the notification of conformity assessment bodies. Furthermore, relevant implementing and delegated acts were adopted and are being prepared, a first set of comprehensive guidelines was published and others are in preparation, and work has also been ongoing on standards.

The **Cyber Solidarity Act (CSoA)**[24] lays down measures to strengthen capacities in the EU to detect, prepare for and respond to cybersecurity threats and incidents. Since its entry into force in February 2025, work has been ongoing to operationalise its key components, including the European Cybersecurity Alert System, the Cybersecurity Emergency Mechanism, and the EU Cybersecurity Reserve.

Concerning the **Cybersecurity Act (CSA)**[25], besides progress in certification activities, the most relevant development has been the proposal to revise it. The proposal for a CSA2[26] is intended to streamline certification, to introduce a framework for the attestation of cybersecurity skills, to clarify and strengthen ENISA's role and to establish a framework for the security of trusted ICT supply chains.

The proposal for **CSA2**, as well as the proposal for **targeted amendments** referred to above, are part of the **Cybersecurity Package** proposed by the EC in January 2026.

The **eIDAS 2.0 Regulation**[27], in force since May 2024, is moving into implementation. Implementing acts adopted during the period 2024 to 2026 further specify frameworks for European Digital Identity Wallets and Trust Services. MSs are expected to deploy wallets by the end of 2026.

---

16 European Commission, *Digital Omnibus Regulation proposal*, 2025, available at: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal (accessed 2 June 2026).

17 European Commission, *EU Action Plan on Cybersecurity and Artificial Intelligence*, 2026, available at: https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence (accessed 15 September 2026).

18 NIS2 Directive (Directive (EU) 2022/2555), available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (accessed 3 June 2026).

19 NIS Cooperation Group, *EU ICT Supply Chain Security Toolbox*, 2026, available at https://ec.europa.eu/newsroom/dae/redirection/document/124123 (accessed 2 June 2026).

20 Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the proposal for a revised Cybersecurity Act (Cybersecurity Act 2), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0013 (accessed 15 September 2026).

21 European Commission, *Commission Implementing Regulation (EU) 2024/2690 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers*, 2024, available at: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng (accessed 4 June 2026).

22 European Council, *Council Recommendation on an EU blueprint for cyber crisis management*, available at: http://data.europa.eu/eli/C/2025/3445/oj (accessed 18 August 2026).

23 Regulation (EU) 2024/2847 of the European Parliament and of the Council on *horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*, available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj (accessed 4 June 2026).

24 Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 *establishing measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (Cyber Solidarity Act)*, available at: https://eur-lex.europa.eu/eli/reg/2025/38/oj (accessed 4 June 2026).

25 Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and *on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj (accessed 4 June 2026).

26 European Commission, *Proposal for a Regulation on ENISA, the European cybersecurity certification framework and ICT supply chain security (Cybersecurity Act 2) (COM(2026) 11 final)*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0011 (accessed 4 June 2026).

27 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards *establishing a framework for a European Digital Identity (eIDAS 2.0)*, available at: https://eur-lex.europa.eu/eli/reg/2024/1183/oj (accessed 4 June 2026).

2.2.2 Sector-specific developments

Sector-specific initiatives have also continued.

Telecommunications. The **EU 5G Cybersecurity Toolbox**[28] (2020) continues to guide coordinated measures to mitigate risks in 5G networks. The EC has also presented a proposal for a **Digital Networks Act**[29], which would simplify the legal framework for digital infrastructures by merging several acts[30].

Finance. The **Digital Operational Resilience Act** (DORA)[31], a *lex specialis* of NIS2 for the financial sector, began being applied in January 2025. It introduces, among others things, the EU Systemic Cyber Incident Coordination Framework (EU-SCICF) and establishes a dedicated 'Oversight Framework' for critical ICT third-party service providers for financial entities[32].

Health. In 2025, the EC adopted a **European action plan on the cybersecurity of hospitals and healthcare providers**[33]. Moreover, the 2025 **European Health Data Space Regulation**[34], for the use and exchange of electronic health data across the EU, entered into force on 26 March 2025, marking the beginning of the transition phase towards application.

Energy. The 2024 **Network Code on Cybersecurity (NCCS)**[35], which addresses the cybersecurity of cross-border electricity flows, has moved into the operational phase.

Transport. Cybersecurity developments are progressing across transport modes, including aviation[36], road transport[37] and maritime[38]. The sector is also shaped by horizontal EU frameworks, such as the Joint Communication on Military Mobility[39].

Space. The EC adopted a proposal for an EU Space Act[40] , currently in the co-decision process, to introduce a framework for the resilience of space infrastructure.

2.2.3 Cross-cutting EU initiatives relevant to cybersecurity

Cybersecurity is also underpinned by a broader set of EU strategies, such as the **European Preparedness Union Strategy**[41], the **ProtectEU Internal Security Strategy**[42], the **International Digital Strategy**[43] and the **Quantum Europe Strategy**[44].

Following several disruptive events, three action plans have been presented, the **EU Action Plan on Cable Security** (2025)[45] to tackle the security of critical submarine cables for communications or energy transmission, the **EU Action Plan on Drone and Counter-Drone Security** (2026)[46] and the **EU Action**

28 European Commission, *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, 2020, available at https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures (accessed 2 June 2026).

29 European Commission, *Proposal for a Regulation on the Digital Networks Act (DNA)*, available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-digital-networks-act-dna (accessed 4 June 2026).

30 The DNA is merging four legal acts into one directly applicable Regulation, replacing the European Electronic Communications Code (EECC), the BEREC Regulation, the Radio Spectrum Policy Programme and the core parts of the Open Internet Regulation.

31 Regulation (EU) 2022/2554 *Digital Operational Resilience Act (DORA)*, available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (accessed 15 September 2026).

32 The framework coordinates responses among financial supervisors, the EU and national authorities during major cross-border cyber threats.

33 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European action plan on the cybersecurity of hospitals and healthcare providers*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0010 (accessed 15 September 2026).

34 Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the *European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847*, available at: https://eur-lex.europa.eu/eli/reg/2025/327/oj (accessed 15 September 2026).

35 Commission Delegated Regulation (EU) 2024/1366 establishing a Network Code on Cybersecurity for the Electricity Sector (NCCS), available at: https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj (accessed 4 June 2026).

36 Commission Implementing Regulation (EU) 2023/203, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R0203 ; Commission Delegated Regulation (EU) 2022/1645, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1645 ; and Commission Delegated Regulation (EU) 2025/22, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0022 (accessed 15 September 2026).

37 Commission Delegated Regulation (EU) No 2025/1535 supplementing Regulation (EU) No 2024/2847 with regard to an *exclusion from the application of that Regulation for certain products with digital elements falling within the scope of Regulation (EU) No 168/2013*; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions No 2025/95, *Industrial Action Plan for the European automotive sector*, 2025, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0095 (accessed 15 September 2026).

38 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Commission, *EU Industrial Maritime Strategy*, 2026, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026DC0111 (accessed 15 September 2026).; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *EU Ports Strategy*, 2026, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026DC0112 (accessed 15 September 2026).

39 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council on Military Mobility*, 2025, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0846 (accessed 15 September 2026).

40 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the *safety, resilience and sustainability of space activities in the Union (Space Act)*, 2025, available at: https://defence-industry-space.ec.europa.eu/eu-space-act_en (accessed 4 June 2026).

41 Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the *Regions on the European Preparedness Union Strategy*, 2025, available at: https://commission.europa.eu/topics/preparedness_en (accessed 4 June 2026).

42 Communication from the Commission to the *European Parliament and the Council on the European Internal Security Strategy (ProtectEU)*, 2025, available at: https://home-affairs.ec.europa.eu/news/commission-presents-protecteu-internal-security-strategy-2025-04-01_en (accessed 4 June 2026).

43 Joint Communication to the European Parliament and the Council, *The International Digital Strategy for the European Union*, 2025, available at: https://digital-strategy.ec.europa.eu/en/policies/international-digital-strategy (accessed 4 June 2026).

44 Communication to the European Parliament and the Council: *Quantum Europe Strategy – Quantum Europe in a Changing World*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0363 (accessed 4 June 2026).

45 Joint Communication to the European Parliament and the Council, *EU Action Plan on Cable Security*, 21 February 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0009 (accessed 4 June 2026).

46 European Commission, Communication from the *Commission to the European Parliament and the Council on an Action Plan on Drone and Counter-Drone Security*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026DC0081 (accessed 4 June 2026).

Plan on Cybersecurity and Artificial Intelligence[47].

Regarding physical resilience, the 2022 **Critical Entities Resilience (CER) Directive**[48] establishes a framework for the resilience of critical entities against physical and hybrid risks, complementing NIS2.

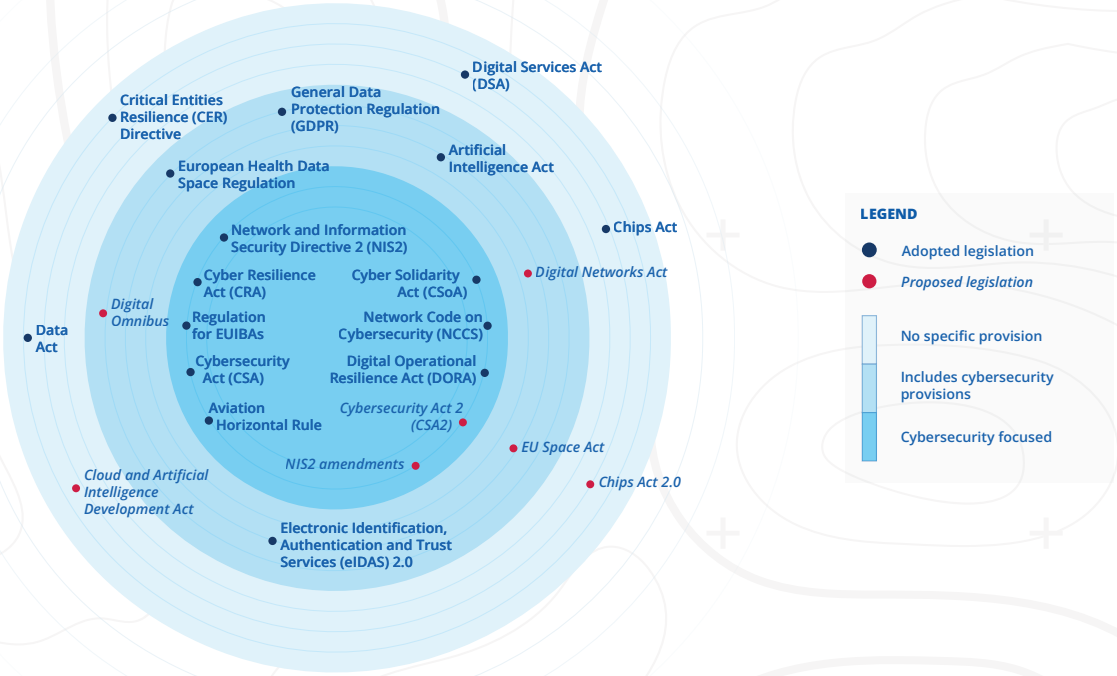
On the international stage, cyber diplomacy efforts are continuing, in particular under the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (**EU Cyber Diplomacy Toolbox**)[49] and the EU continues to work with partners to advance shared interests in cybersecurity policy[50].

In the same vein, other relevant horizontal frameworks in the wider digital policy context exist, including the **General Data Protection Regulation (GDPR)**[51], the **AI Act**[52], **the Digital Services Act (DSA)**[53], and the **Data Act**[54]. The DSA and the Data Act do not contain cybersecurity provisions in a strict sense, but they do contribute to the broader EU digital resilience ecosystem.

In June 2026, the EC presented a package on **technological sovereignty** to strengthen Europe's digital autonomy and resilience. The package encompasses four initiatives. These are the **Chips Act 2.0**, the **Cloud and AI Development Act (CADA)**, the **EU Open Source Strategy**[55], and a **Strategic Roadmap for Digitalisation and AI in Energy**[56].

Looking forward, a **Quantum Act** has also been announced[57] with one of its dimensions expected to focus on ensuring the security and resilience of quantum supply chains.

Figure 4: *EU Policy landscape based on cybersecurity provisions*



---

47 European Commission, *EU Action Plan on Cybersecurity and Artificial Intelligence*, available at: https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence

48 *Directive (EU) 2022/2557 Critical Entities Resilience Directive – CER Directive*, available at https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed 4 June 2026).

49 *EU Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox)*, available at: https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/ (accessed 4 June 2026).

50 The EU has Cyber Dialogues with the US, Ukraine, the United Kingdom, Japan, India, the Republic of Korea and Brazil. Cybersecurity is also discussed in the Digital Partnerships with Japan, the Republic of Korea, Singapore and Canada and the Digital Dialogues with Brazil, Mexico, Argentina, Australia and the Western Balkans. More info available at: https://ec.europa.eu/newsroom/dae/redirection/document/116453 (accessed 4 June 2026).

51 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (accessed 4 June 2026).

52 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised *rules on artificial intelligence* and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed 4 June 2026).

53 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a *Single Market for Digital Services* and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (accessed 4 June 2026).

54 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised *rules on fair access to and use of data* and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), available at: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (accessed 4 June 2026).

55 https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy (accessed 8 October 2026).

56 https://energy.ec.europa.eu/topics/eus-energy-system/digitalisation-energy-system_en#strategic-roadmap-for-digitalisation-and-ai-in-energy (accessed 8 October 2026).

57 European Parliament, *Legislative Train Schedule - Quantum Act*, available at: https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-quantum-act (accessed 8 September 2026).

2.3 The EU-Cybersecurity Index: High-level findings

In line with Art. 18(3) of NIS2, ENISA continues to further develop and improve the EU-Cybersecurity Index (EU-CSI). The Index comprises the methodology and the indicators needed to support the aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the EU.

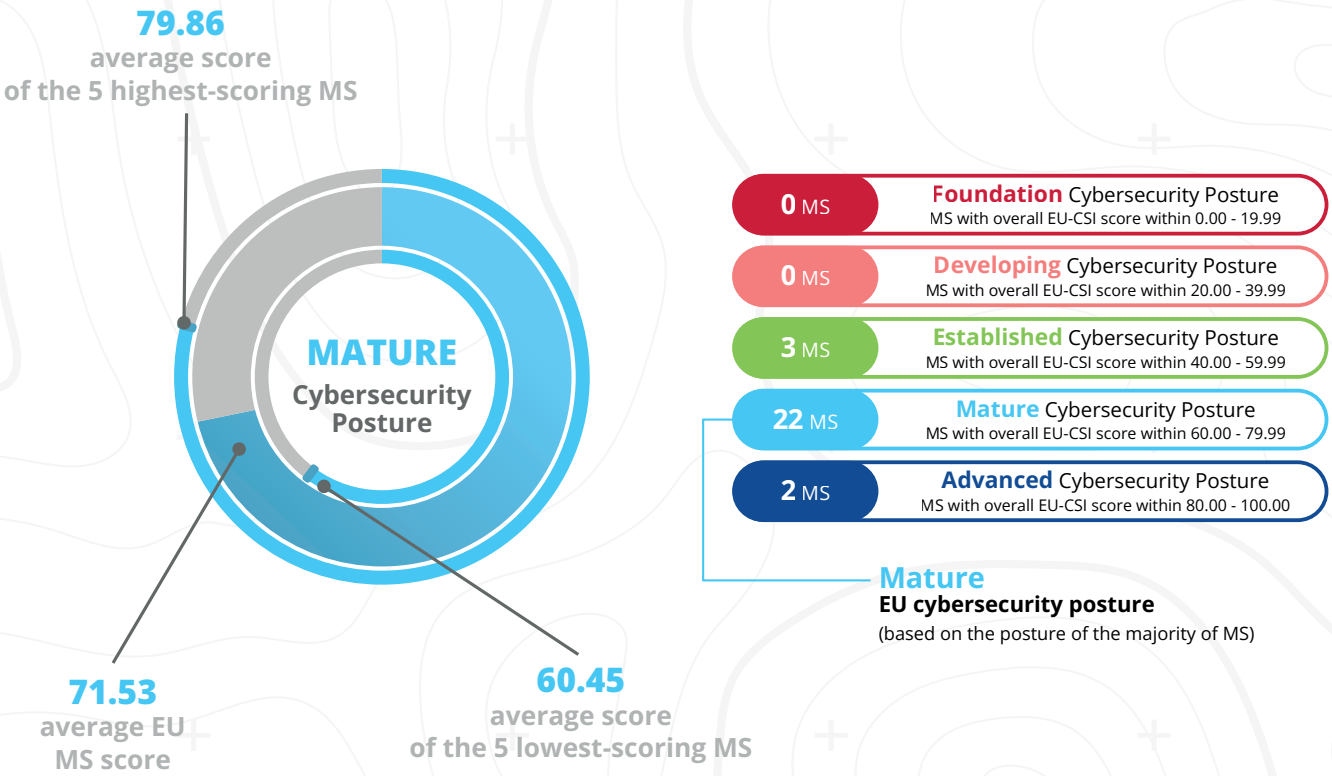
The framework analyses the cybersecurity posture of the EU covering multiple perspectives, including the state of policy development and implementation, the ability of the public and private sectors to recognise threats and prevent incidents, and the capability to carry out operations to ensure resilience.

The EU-CSI was revised for the 2026 edition, mainly by prioritising simplicity and improving the framework's clarity and cohesion as well as the quality and relevance of the indicators. Furthermore, the revised EU-CSI framework features five cybersecurity posture levels to facilitate the reading of the results. The data collection phase took place at the end of 2025.

2.3.1 EU-CSI EU-Wide Results

Based on the aggregated results, **the overall EU average value of the Index 2026 is 71.53 points**[58] (on a scale from 0 to 100) with **the majority of MS achieving a mature cybersecurity posture level or above**. The average score of the five highest scoring MS is 8.33 points above the EU average, and the average score of the five lowest scoring MS is just 11.08 points below the EU average. **The aggregated Index results indicate a quite mature cybersecurity posture and an overall alignment of the MS within the EU**.

EU Cybersecurity Index 2026



58 The numerical results of the revised Index are not directly comparable with those of the previous iteration due to changes in the framework.

2.3.2 Selected High-level Findings



There seems to be convergence among MS with most of them achieving a mature cybersecurity posture, which signals progress towards achieving a *common* high level of cybersecurity. This is further reinforced by the fact that even the average of the five lowest scoring MS is relatively high.



Policy implementation at the national level is progressing across the EU. The majority of MS achieved a mature or advanced posture on the coverage and implementation of objectives in national cybersecurity strategies (66.72 points), highlighting their increased alignment. There are, however, still gaps between strategic intent and actual execution in some areas.

A high maturity posture for the majority of MS was also observed in the implementation of incident reporting provisions (71.06 points) and in vulnerability disclosure policies (79.80 points). However, the latter is one of the indicators where MS are the least aligned, reflecting uneven progress. Despite the high EU average maturity, the increased risk introduced by advances in AI further highlights the importance of progressing the implementation of policy even further. Additionally, a mature posture was observed on the cooperation between competent authorities and/or bodies at national level (75.68 points), and the definition and compliance of cybersecurity risk management measures for essential and important entities (67.96 points), as well as the supervision of essential and important entities (68.33 points). With the latter two indicating that there is room for further development.



Essential and important entities present a mature posture overall though there are some areas requiring improvement. Almost all MS achieved an advanced posture on practices for the management of supply chains adopted by their essential and important entities (89.91 points). Yet further improvement is possible considering the relevance of the topic. At the same time, almost all MS are at the developing level of maturity when participation by their essential and important entities in peer-to-peer information sharing activities (26.30 points) is considered. This is one of the most aligned indicators, and it shows that there is room for improvement to enhance information sharing and collaboration.



The maturity of CSIRTs still stands out as an area of potential growth. The indicator measuring the maturity level of CSIRTs is 54.76 points, and it is one of the least aligned indicators, indicating that, in multiple MS, the average maturity of CSIRTs is either low or not assessed.



The presence of cybersecurity in education especially at the lower levels can be further improved. Actions to promote and enhance cybersecurity in higher levels of education are being undertaken by most MS (73.59 points), with 21 MS showcasing a mature or better posture. However, data also suggests that cybersecurity-related curricula in lower education (primary and secondary levels) is lagging behind (54.44 points) with only 12 MS achieving a mature or advanced posture.

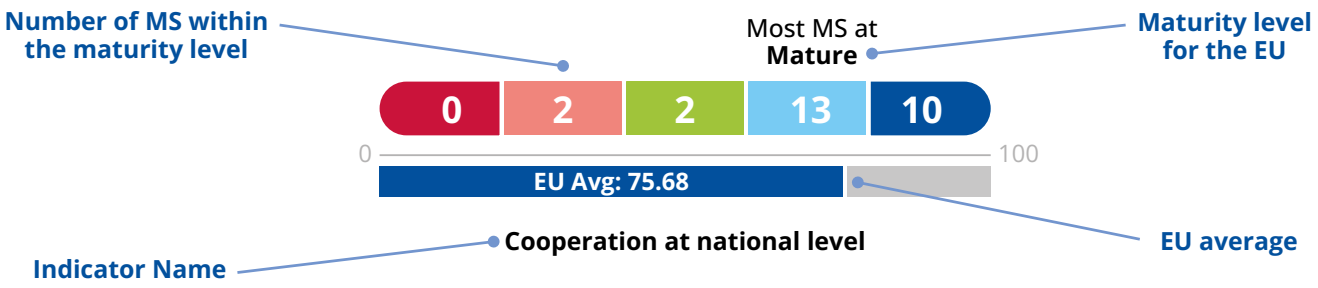


National certification ecosystems are split between mature and less mature. The indicator on national certification capabilities shows that MS are on both edges of the maturity scale – 13 MS on the foundation or developing levels and 14 MS on the mature or advanced levels – resulting in a score in the middle of the scale (55.56 points). This is one of the least aligned indicators and it indicates that there are gaps in capabilities between MS.



Increasing coherence in the R&I landscape. Most MS achieved an advanced posture in the topic of priorities and initiatives in cybersecurity R&D (79.24 points). This indicates that the majority of MS are taking appropriate action to identify, define, promote and support cybersecurity research and development priorities both at the national and at the international level.

A selection of the EU-CSI indicators is included in various sections of the report, presenting the EU's maturity level, the average EU score, as well as the number of MS on each maturity level, as in the following example.



The posture level for each indicator corresponds to the level in which the majority of the MS are concentrated.

Foundation	Developing	Established	Mature	Advanced
majority of MS with scores within	majority of MS with scores within	majority of MS with scores within	majority of MS with scores within	majority of MS with scores within
0.00 — 19.99	**20.00 — 39.99**	**40.00 — 59.99**	**60.00 — 79.99**	**80.00 — 100.00**

III.

Main directions of the EU cybersecurity ecosystem



SHIFTING TO **EFFECTIVE IMPLEMENTATION**

3.1 Shifting to effective implementation



Summary

The process of transposing NIS2 has been substantial and is still ongoing.

MS are dealing with a broader set of essential and important entities than under NIS1. They are developing or expanding supervisory governance and processes, as well as frameworks for risk management, while establishing more structured cooperation amongst national authorities and more structured processes for incident reporting.

The results of these efforts are now becoming visible. More MS report that they will update their lists of relevant important and essential entities at least every two years and that they have defined a process to identify entities that are micro or small enterprises. Risk management obligations are now generally in place. Furthermore, cooperation at the national level and with frameworks such as DORA and CER is mostly established. National cybersecurity strategies show strong alignment with NIS2 objectives, despite some gaps in more complex areas, notably coordinated vulnerability disclosure (CVD), active cyber protection, mutual assistance and supply chain security.

National transpositions of NIS2 have not been fully implemented in MS and the same scale-up that has driven progress is also placing pressure on national competent authorities and/or bodies, while cross-border and cross-legislative aspects become more relevant.

The variation in frameworks for risk management and supervision among MS has an impact on companies operating across borders. This is true also for incident reporting, which is further complexified by the existence of several EU acts requiring reporting to different authorities.

Given the complexity of the EU cybersecurity policy landscape, its effectiveness relies largely on the way it is implemented. As discussed above, implementation is progressing in parallel with new legislative developments, at times integrating lessons learnt from operational experience. This pattern is observable especially in the context of NIS2. MS have transposed NIS2 at different times, the majority after the transposition deadline of October 2024, while a few are still in the legislative process. Early adopters are sharing their experience, identifying areas where coherent implementation is challenging, especially because of cross-border or cross-legislative aspects. Differences in implementation stages and modes affect how MS engage with each other and contribute to a high *common* level of cybersecurity in the EU. As such, EU and national efforts are striving to achieve minimum harmonisation and, in general, to create the conditions for an effective implementation of NIS2 through simplification.

This section reports on the evolution of and the challenges in areas of NIS2 previously identified in 2024, where national implementation is particularly complex. It also reports on the alignment of national strategies. Finally, the section gives a brief overview of the state of implementation of two other core legislative acts, the CSoA and CRA, that are in an earlier stage of implementation with respect to NIS2.

3.1.1 Supervision

The supervision of essential and important entities is a foundational step in the implementation of NIS2 and is regarded as one of the trickiest areas to operationalise. **The EU-CSI 2026 indicates that MS are equally spread across an established, mature and advanced posture, with an average score of 68.33.**

Data on the share of essential and important entities for which national authorities collect minimal information (e.g. name and address) show persistent disparities. Approximately one third of MS collect this information from 81% to 100% of entities and a quarter of MS from 0% to 20% of such entities. That said, there has been clear progress since 2024 and, although all MS are not yet at the same level, most are improving. In 2024, the number of MS collecting information in the above ranges were 3 and 12 respectively.



Supervision of essential and important entities

Equally encouraging is the fact that almost all MS (25) update their list of essential and important entities at least every two years. Additionally, 15 of them report doing so even more frequently.

There has also been clear progress on the identification of smaller entities. The number of MS that have defined a process to identify essential and important entities that are micro or small enterprises has increased from 15 to 21 since 2024. The number of MS that have defined and implemented such a process has grown from 11 to 14 over the same period. This points to a stronger effort towards a proportionate approach to the implementation NIS2.

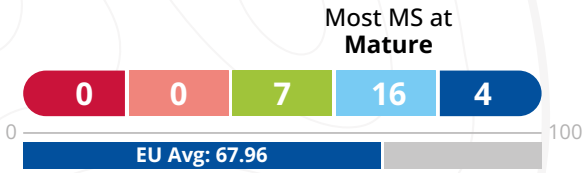
The share of essential and important entities subject to supervisory tasks by authorities has only slightly shifted since 2024. In 2026, as in 2024, approximately one third of MS (10 in 2024 and 9 in 2026) subjected between 81% and 100% of essential and important entities to the supervisory measures listed in Art. 32(2) of NIS2. Approximately a quarter of MS (6 in 2024 and 8 in 2026) subjected between 0% and 20% of essential and important entities to these measures. For some MS, this may reflect a more targeted supervisory model and/or practices derived from lessons learnt from MS that are more advanced in the implementation of NIS2. For others, it might reflect an earlier stage of transposition.

Broader challenges underline these findings. MS have expressed difficulties in defining which entities fall within the scope of specific NIS2 sectors. Accordingly, the proposed NIS2 targeted amendments clarify the perimeters of sectors with an impact on, for example, healthcare services, electricity producers, hydrogen operators and subsea cable infrastructure. In addition, the sharp increase in entities within the scope of NIS2, with respect to NIS1, had resulted in growing complexity in coordination and administrative workloads, putting significant pressure on national supervisory systems. MS reported difficulties in making entities, especially those newly within the scope of NIS2, aware of their obligations. Lastly, different supervisory frameworks across MS and a lack of mechanisms for mutual recognition among them affect entities operating cross-border, as they can be subject to different rules.

Good practices in Member States

Turning regulatory implementation into a cooperative process through formal sectoral working groups, regular engagement with regulated entities, dedicated support desks, extensive FAQs, and promotion of financial support for cybersecurity investments. This helps organisations resolve practical questions early, and supports more consistent compliance, particularly among SMEs and newly regulated entities.

3.1.2 Cybersecurity risk management measures



Definition and compliance of cybersecurity risk management measures for essential and important entities

The EU-CSI 2026 indicates that the majority of MS have a mature posture with respect to the definition of and compliance with risk management measures for essential and important entities. This is a slight improvement with respect to 2024. All 27 Member States now mandate measures for the management of risk in essential and important entities as required under Art. 21 of NIS2. This improvement concerns measures related to supply chain security, vulnerability handling and disclosure, advanced authentication methods, and the use of cryptography for which approximately seven more MS have mandated requirements. In addition, at the national level, many MS have adopted national frameworks for compliance with NIS2. These include cybersecurity measures, setting-up voluntary compliance schemes linked to NIS2 and mapping NIS2 requirements to existing standards. Still, since not all MS had transposed NIS2 when data was being collected, it is likely that mandatory risk management requirements had been put in place also through other means. At the EU-level, the Commission Implementing Regulation on cybersecurity risk management for specific categories of entities providing digital services was adopted at the end of 2024[59].

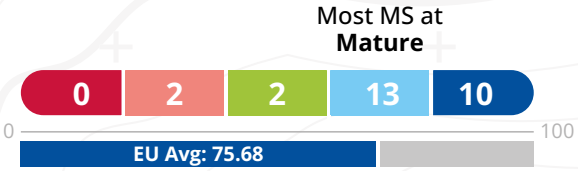
Good practices in Member States

Security requirements introduced in secondary legislation are mandated to be proportionate, taking an entity's criticality, sector, size and level of cybersecurity maturity into account. Entities are required to first implement a set of basic security measures within a short timeframe, differentiated for essential and important entities, followed by strengthened requirements over a longer period. This provides SMEs and less mature sectors with a feasible pathway to compliance.

MS are also putting mechanisms in place to actively check compliance. With respect to 2024, more countries also rely on self-assessments (17 MS, up from 9) and implement follow-up actions based on findings. This suggests that **MS are gradually moving towards more formal and structured ways for checking compliance. However frameworks for security measures vary between MS and this has an impact on companies operating across borders**. These entities are required to prove compliance in several different ways. Addressing such differences is likely to become a growing priority in the future.

3.1.3 Information sharing and incident reporting

Effective information sharing depends on close coordination between relevant actors, as cyber threats and incidents rarely remain limited to a single sector or authority and often require a coordinated response.



Cooperation at national level

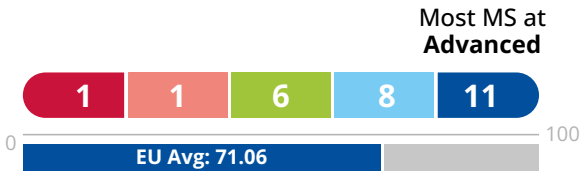
The EU-CSI indicates that the majority of MS have a mature posture with respect to cooperation at the national level, encompassing both cooperation among competent authorities, CSIRTs and SPOCs, and cooperation with authorities designated under other EU legal acts, e.g. for regular information exchange on cyber incidents and threats.

National-level cooperation among competent authorities, CSIRTs and SPOCs mandated by NIS2 has reached a more mature level. This was brought about by continuous efforts to formalise and refine mechanisms for coordination. Since 2024, three additional MS have formally documented, or established, or updated their mechanisms for cooperation, bringing the total to 23 MS. **NIS2 also requires cooperation between those bodies and the competent authorities established under other EU frameworks**, including DORA, the CER Directive and eIDAS. **Cooperation under these frameworks continues to develop at different speeds**. Cooperation between NIS2 and DORA and CER authorities has progressed the most. Regular information exchange on cyber incidents and threats with the competent authorities responsible for DORA and CER has been or is being established in respectively 22 and all MS respectively, increasing by five MS since 2024. Cooperation with EECC and eIDAS authorities has remained stable (18 MS and 19 MS, respectively).

A key area of cooperation concerns the sharing of

59 European Commission, *Commission Implementing Regulation (EU) 2024/2690 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, providers of online search engines and of social networking services platforms, and trust service providers*, available at https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng (accessed on 20/09/2026)

information about cybersecurity incidents notified to the different competent authorities. Several EU legal acts require the reporting of incidents to relevant competent authorities by entities within the scope of those acts. **MS report that thresholds for what constitutes a significant incident can be unclear to entities and can be interpreted differently across MS**. This means that comparable events could be reported in one country but not in another. Similarly, the lack of clear procedures for the notification of cross-border incidents and of a standard procedure to characterise an incident as such results in a lack of a proper sharing of information. Notifications can also serve multiple purposes at once, from operational incident response and situational awareness to statistical analysis and regulatory oversight, and it might not always be clear which of these should take precedence in each case. However, when purposes compete, the administrative handling of reports can place additional strain on incident-response functions, with resources spent on processing notifications rather than acting on them. These challenges are further compounded by capacity constraints in several MS and create complexity for entities within the scope of different obligations for reporting incidents.



Incident reporting implementation

Despite these challenges, the **implementation of incident reporting obligations is advanced**. To support the implementation of these reporting obligations, most MS (22 MS) have defined and documented a national taxonomy for the classification of cyber incidents, as well as thresholds for their evaluation (17 MS). At the same time, measures to ensure the confidentiality and integrity of information shared through reporting channels are in place in almost all MS (26 MS). Attention is also increasingly turning to the effectiveness of these frameworks, with around two thirds of Member States having started to assess their functioning, for example through indicators measuring whether incidents are reported via the appropriate channels and within the required timeframes (16 MS).

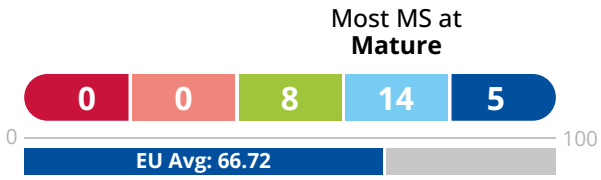
Work on streamlined procedures facilitating reporting across multiple legislative frameworks (e.g. NIS2, DORA or GDPR) is still ongoing in several Member States (16 MS) and 8 MS report having a harmonised procedure (e.g., with common reporting templates) for sectorial incident reporting scheme across different legislations.

Infobox: Incident Reporting In Practice



A look at the trends in incident reporting provides additional insights on how incident reporting frameworks function in practice. The Cybersecurity Incident Reporting and Analysis System (CIRAS)[60] has been collecting cybersecurity event reports from MS for many years and under different legislations, in particular the EU Electronic Communications Code (ECCC Directive 2018/1972), the Regulation on electronic identification and trust services (eIDAS1 Regulation 910/2014) and NIS1. The reporting provisions under these legislations have generally converged under NIS2, hence the data collected in 2025 covers solely NIS2. The total number of NIS2 events reported in 2025 was 1.954. This was an increase of almost 30% in reported events compared with 2024, when 1.508 events were reported. However, the number of MS submitting data through CIRAS has decreased to an average of 20 in 2025 compared to 24 in 2024. This might be related on the one hand to an increased number of sectors within the scope of NIS2 and, on the other hand, to the on-going transposition of NIS2 in several countries[61].

3.1.4 National cybersecurity Strategies



Coverage and implementation of objectives in national cybersecurity strategy

Under Art. 7 of NIS2, MS are required to develop and adopt a National Cyber Security Strategy (NCSS), providing for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures. Since 2017, all MS have a NCCS in place.

60 ENISA, Cybersecurity Incident Reporting and Analysis System (CIRAS) Website, available at: https://ciras.enisa.europa.eu (accessed 15 September 2026).
61 ENISA, *2025 Annual overview: NIS2 Cybersecurity Incident Reporting*, available at https://ec.europa.eu/newsroom/dae/redirection/document/132389 (accessed 22 September 2026).

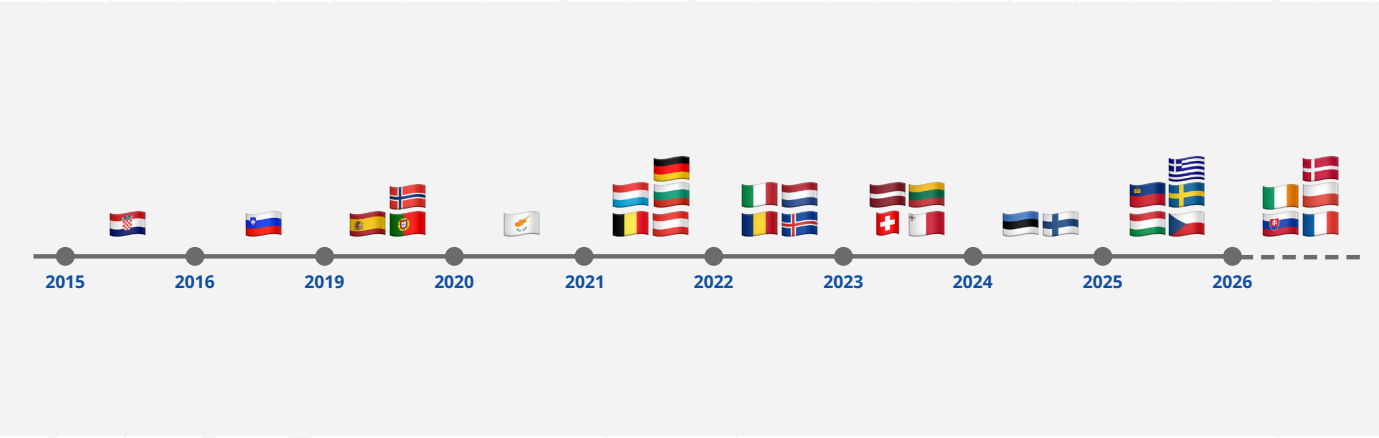


Figure 5: *Adoption year of the latest NCSS for each MS*[62]
Each flag marks the year each Member State adopted its latest national cybersecurity strategy.

While in 2024 four MS were still on their first-generation strategy, current data show that almost all MS have now updated their NCSS to at least a second version, with 12 already on their third or later revision. Moreover, apart from the latest official NCSS, MS may have defined updated cybersecurity-related objectives or actions as part of other strategic documents (e.g. other National Strategies or National Action Plans) that are not visible on the timeline above.

Although MS can have different priorities reflecting their national context, as already observed in the 2024 Report, **NCSSs show a strong degree of alignment**. Most objectives identified as strategic by ENISA are included in the NCSS documents of a large majority of MS[63].

However, areas that are more complex or were introduced by NIS2 show a lower uptake in NCSSs and in action plans. This is reflected in the EU-CSI indicator 'Coverage and implementation of objectives in National Cybersecurity Strategies', which measures the coverage and implementation of NCSS's strategic objectives, including the presence of action plans and mechanisms for adaptive governance. These are, for example, coordinated vulnerability disclosure (CVD), active cyber protection, mutual assistance and supply chain security. These areas show the widest gaps between strategic intent and actual execution. In particular, supply chain security shows a slightly higher degree of uptake relative to the previous reporting period, but it remains low compared to other areas. This likely reflects the fact that supply chain security is particularly complex to address at national level, as it requires identification of several dependencies, such as cross-border and cross-sector dependencies, and stronger coordination among public authorities.

To support the adoption of strategies that jointly achieve and maintain a high level of cybersecurity across the EU, in line with NIS2, ENISA, in early 2026, with the support of the NIS Cooperation Group, revised the National Capabilities Assessment Framework (NCAF). This allows MS to undertake a self-assessment of their level of maturity by evaluating their NCSSs[64].

62 The timeline is based on data up to 7th of October 2026. The latest up-to-dated data are available on ENISA's NCSS interactive map website, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies (accessed 15 September 2026).

63 ENISA, *National Cybersecurity Strategies Interactive Map*, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies (accessed 15 September 2026).

64 ENISA, *National Capabilities Assessment Framework 2.0*, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncaf (accessed 15 September 2026)

Infobox:
Peer Reviews Of National Cybersecurity Frameworks

Art. 19 of NIS2 introduces voluntary peer reviews among MS to enhance mutual trust and improve cybersecurity capabilities across the EU.

Coordinated through NIS CG with the assistance of the EC and ENISA, these peer reviews can assess various aspects of national cybersecurity frameworks. Their primary objective is to promote mutual learning through the exchange of experiences and best practices, thereby strengthening the EU's overall cybersecurity posture.

In 2025 a pilot peer review was conducted, in which Greece, Luxembourg and Italy acted as Reviewer Peers of Cyprus. The review covered the implementation of measures to manage risk in accordance with NIS2 and the capabilities of competent authorities as well as cross-border and cross-sector supply-chain security.

The overall assessment concluded that Cyprus had established a mature cybersecurity framework and had demonstrated strong alignment with EU legislation, and international standards. The governance structure had integrated public-private collaboration, sectoral coordination and active engagement at the EU-level.

In 2026, a second peer review was conducted, with the Slovak Republic participating as a Learner Peer and the Czech Republic and Hungary acting as Reviewer Peers. The review focused on the capabilities of the competent authority in carrying out its tasks, particularly in the areas of cybersecurity regulation, supervision and law-making.

The overall assessment concluded that the Slovak Republic had demonstrated a mature cybersecurity governance and operational implementation framework while identifying good practices and areas for further improvement. During the peer review it was also confirmed that Slovakia has established effective governance and supervisory mechanisms supported by an appropriate legal framework and clearly assigned institutional responsibilities.

Both reviews highlighted common challenges faced by multiple MS, including increasing supervisory demands following the implementation of the NIS2 Directive and the need to ensure sufficient resources and efficient approaches to cybersecurity supervision. On a more general level, they confirmed the usefulness of mutual learning and called for a structured replication of the peer-review mechanism, informed by the lessons learnt in these first iterations.



In Focus: Implementation of other core legislation
Cyber Solidarity Act (CSoA) | Cyber Resilience Act (CRA)

Since the entry into force of the CSoA[65], in February 2025, work has been ongoing to operationalise its key components, including the European Cybersecurity Alert System and the Cybersecurity Emergency Mechanism.

The **European Cybersecurity Alert System** relies on a federated network of National and Cross-Border Cyber Hubs designed to increase detection capabilities and disseminate actionable early warnings. It addresses cross-border challenges through intelligence sharing. Currently, three cross-border consortia have been established for this purpose and are in the process of becoming operational.

Central to the Cybersecurity Emergency Mechanism is the EU Cybersecurity Reserve, which represents a pool of trusted EU-controlled Managed Security Service Providers (MSSPs). The Reserve is established to assist countries, upon request, in responding to, or providing support for a response to, significant cybersecurity incidents or large-scale cybersecurity incidents, and initiating recovery from such incidents. In accordance with the CSoA, ENISA was tasked with and has established and operationalised the EU Cybersecurity Reserve[66]. The Reserve employs a flexible operational model to ensure the most efficient use of available resources. Funds that are not required for incident response can be used for preparedness services closely related to incident response and incident prevention[67].

Under specific conditions, under Art. 19 of the CSoA, the Reserve can also be used by third countries associated to Digital Europe Programme. The Republic of Moldova became the first among third countries to access the EU Cybersecurity Reserve. As of June 2026, Ukraine can also activate emergency EU cyber support to respond to significant/equivalent of large-scale cybersecurity incidents[68].

The Reserve builds on the best practices and processes of the Support Action Programme. This programme has been reinforcing national preparedness and response capabilities, first with a pilot in 2023 (with an allocation of EUR 15 million) and then with a second phase spanning 2024 to 2026 (with an allocation of more than EUR 20 million). The Action has financed an extensive portfolio of cybersecurity services tailored for MS. Since January 2024, over 400 services have been delivered, mainly penetration testing and cybersecurity exercises.

The CRA has transitioned from the legislative phase into the operational implementation stage, with the 2026 calendar dictating key steps leading to full applicability as of December 2027.

Concretely, the EC has exercised its delegated powers to define the technical requirements. Notable milestones include two delegated regulations, adopted in 2025 and 2026, one excluding certain vehicles from the scope of the CRA[69] and one specifying the terms and conditions under which CSIRTs could delay the dissemination of vulnerabilities and the notification of incidents. In addition, in 2025, the EC adopted a Commission Implementing Regulation containing a technical description of important and critical products with essential elements[70].

Standardisation plays an important role in facilitating implementation of the CRA and the presumption of conformity with its requirements. Simultaneously, the work is on-going to establish a presumption of conformity on the basis of the EU cybersecurity certification scheme on Common Criteria (EUCC), after the adoption of a delegated act which could be expected by the end of 2026.

On the Member States' side, since 11 June 2026 Member States are required to designate their notifying authorities, a prerequisite for the establishment of a network of Conformity Assessment Bodies by 11 December 2026. **Since 11 September 2026, actively exploited vulnerabilities are being reported to the CRA Single Reporting Platform (See** section 3.4**).**

---

65 Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to *strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents* and amending Regulation (EU) 2021/694 *(Cyber Solidarity Act)*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0038 (accessed 9 June 2026).

66 Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02021R0694-20251223 (accessed 9 June 2026).

67 ENISA, *EU Cybersecurity Reserve*, available at: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cybersecurity-reserve (accessed 9 June 2026).

68 European Commission, *EU provides cyber support to Ukraine against major attacks*, https://digital-strategy.ec.europa.eu/en/news/eu-provides-cyber-support-ukraine-against-major-attacks (accessed 6 July 2026).

69 European Commission, *Delegated Regulation (EU) 2025/1535 supplementing Regulation (EU) 2024/2847 of the European Parliament and of the Council with regard to an exclusion from the application of that Regulation for certain products with digital elements falling within the scope of Regulation (EU) No 168/2013 of the European Parliament and of the Council*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501535 (accessed 4 July 2026).

70 European Commission, *Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council*, available at https://eur-lex.europa.eu/eli/reg_impl/2025/2392/oj/eng (accessed 15 September 2026).

Policy Recommendations

The main message of the 2024 Report on the State of Cybersecurity in the Union remains: the success of EU legislation will depend to a great extent on the effectiveness of its implementation. For NIS2, building on the progress already achieved, focus should be put on smoothening cross-border and cross-legislative aspects so that entities operating across MS face a coherent, workable and seamless environment.



Key recommendations:

- **[ENISA]** should support MS in their supervisory tasks, namely by sharing best practices on governance models and optimal approaches enabling mutual assistance, especially in cross-border cases.
- **[ENISA and the NIS Cooperation Group]** should prioritise supporting SMEs that are within the scope of NIS2 and newly identified operators by assisting MS in raising awareness on policy requirements and providing guidance and tools.
- **[The EC]** should work with relevant stakeholders to help accelerate the work towards the operationalisation of EU responses to vulnerability handling and management requirements across legislations.

Other recommendations:

- **[MS]** should support the use of a unified framework to evaluate and monitor National Cybersecurity Strategies in order to facilitate the exchange of best practices and reduce strategy-to-implementation divergence, while taking into account national specificities.
- **[The NIS Cooperation Group, with the support of ENISA]** should identify possible simplifications concerning incident reporting across legislations, proposing efficient ways to allow entities subject to different legislations to report incidents, for instance using a common template for various legal acts taking the NIS2 template as a baseline.



ADOPTING A **COMPREHENSIVE OPERATIONAL CAPACITY** IN THE EVENT OF CRISES

3.2 Adopting a comprehensive operational capacity in the event of crises



Summary

The 2025 EU Blueprint for Cyber Crisis Management signals increased national and European commitment towards a joint response at the EU-level to significant incidents. Work will continue towards building a comprehensive operating environment for managing crises, whether focused on cybersecurity or with a cybersecurity component.

The maturity of actors involved in the management of cyber crises is not equal and this fragmented operational maturity can represent a structural risk to EU-wide responses to crises.

Collaboration among and with some actors is still under development. For example, modes of structured cooperation with the military counterparts of EU-level networks (such as the CSIRTs Network and EU-CyCLONe) have not been defined yet. CSIRTs appointed to the CSIRTs Network also show varying maturity levels. The role of the private sector in crisis management is being formally recognised. For example, it is important to exchange information about situational awareness, although this does not happen seamlessly.

The lack of an EU-level comprehensive, common, timely depiction covering all aspects of situational awareness has persisted since the previous Report. Although trust has increased, national capacities, political, economic, policy and technical constraints remain.

To this day, the EU Blueprint for cyber crisis management has never been used in a real-world situation, though iterative testing through structured exercises has yielded valuable insights for its operational refinement. In general, interesting national approaches to cybersecurity exercises are emerging and a high participation in EU-level exercises has been observed but it is not always matched by structured national exercises.

The evolution of cybersecurity crisis management at the EU-level in the last few years has been marked by a sense of urgency derived from the unfolding of multiple conflicts and shifts in the global order. The adoption of the **2025 Council Recommendation on an EU blueprint for cyber crisis management**[71], replacing the 2017 Commission Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises[72], represents a major institutional milestone.

The shift from a *Commission* Recommendation to a *Council* Recommendation is a signal of the heightened European and national commitment towards a European response to significant incidents affecting multiple countries and exceeding the response capacities of a single country. In the same vein, the newly introduced reference to *cyber crisis management* attests the willingness to transcend mere incident response and to focus on the consolidation of a whole operating environment around a crisis.

The 2025 Blueprint clarifies the role and responsibilities of national and EU-level actors in the different phases of crisis management, including stakeholders also from the military domain and the private sector. In addition, it outlines the interactions and information exchange using existing mechanisms for EU and national crisis management that also extend beyond cybersecurity. For example, it complements the EU Critical Infrastructure Blueprint[73] , which is the EU-level mechanism to respond to physical disruptions of critical infrastructure.

3.2.1 EU-level actors

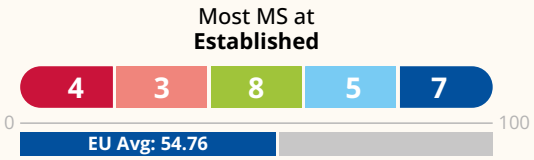
The 2025 Blueprint architecture is based on the principle of shared responsibility: no single actor can manage crises alone and an effective response to a crisis depends on seamless vertical and horizontal coordination across the technical, operational and political tiers.

At the EU-level, the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)[74] emerges as a central actor. It supports the coordinated management of large-scale cybersecurity incidents at the operational level and functions as the intermediary between the technical layer (CSIRTs network) and the political layer (the European Council and the Integrated Political Crisis Response mechanism, for coordinated decision-making for major and complex crises). The CSIRTs network is the primary technical actor and, in most cases, the first activation point in the event of an observed incident. The relationship between EU-CyCLONe and the CSIRTs network is based on structural complementarity and both are expected to cooperate continuously and effectively through procedural arrangements, currently being developed.

In Focus: CSIRTs Network

The CSIRTs network operates at the technical level and is, in the Blueprint's architecture, the main platform for exchanging relevant information about incidents. Among other tasks, the network may facilitate a coordinated response to an incident that has been identified within the jurisdiction of a requesting member. It provides assistance to Member States in managing cross-border incidents and explores further forms of cooperation, including mutual assistance. Overall, it contributes to the development of confidence and trust and promotes swift operational cooperation among MS. Established in 2016 under the NIS Directive, its role was strengthened with the adoption of the NIS2 Directive.

To offer a reference point on the maturity of CSIRTs, the EU-CSI 2026 features a dedicated indicator (CSIRTs Maturity). It shows a fragmented picture, with maturity levels varying considerably across countries. The indicator is based on ENISA's CSIRTs Network Maturity Framework, which assesses the maturity of CSIRT Network Members across key capability areas, such as processes, human resources, tools and organisational cooperation, drawing on the SIM3 model (Security Incident Management Maturity Model).



CSIRT(s) maturity

A score of 100 for this indicator would mean that all appointed CSIRTs that are part of the CSIRTs Network have completed a self-assessment on the basis of ENISA's framework and have achieved an 'expert' maturity level that has also been validated through a peer review. While this goal is particularly ambitious, the heterogeneity across countries is noteworthy as this is one of the EU-CSI indicators where MS are the least aligned.

This is in line with the 2024 Report, which found that only about a third of the Members of the CSIRTs Network were either certified or candidates for (re)certification under Trusted Introducer (TI), meaning that their security incident management procedures, infrastructures and response processes were aligned with internationally recognised standards.

---

71 European Council, *Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management*, available at: https://eur-lex.europa.eu/eli/C/2025/3445/oj (accessed 15 September 2026).

72 European Commission, *Commission Recommendation (EU) 2017/1584 of 19 September 2017 on coordinated response to large-scale cybersecurity incidents and crises*, available at: https://eur-lex.europa.eu/eli/reco/2017/1584/oj/eng (accessed 9 June 2026).

73 Council Recommendation (EU) 2024/4371 on a *Blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance*, available at: https://eur-lex.europa.eu/eli/C/2024/4371/oj/eng (accessed 9 June 2026).

74 EU-CyCLONe was set up on an informal basis in 2020 and then formally established through NIS2.

As neither TI nor ENISA's CSIRTs Network Maturity Framework assess actual operational effectiveness and are voluntary, the picture emerging from the ENISA-CSI 2026 should be interpreted as a structured baseline that could be used to trigger targeted actions to raise the overall maturity and reduce national differences.

Public-Private cooperation

The increasingly important role of the private sector in cyber crisis management is widely recognised. A large portion of critical digital infrastructure is privately owned. Telecommunications, Cloud, Software, Operational Technology and many cybersecurity services are provided by private companies. They are often the first to see threats and incidents, with direct sight of attacks, vulnerabilities and attempts at exploitation, and can therefore provide valuable threat intelligence.

The involvement of the private sector is crucial to minimise disruption and ensure business continuity. Clear public-private communication channels are key for authorities to become aware of incidents and coordinate response, and constant and iterative information sharing reinforces situational awareness. Cooperation with certain sectors, such as operators of digital infrastructure, is particularly important as incidents affecting them are prone to have cross-border effects. The importance of the role of the private sector is underlined in the Blueprint, which indicates that MS should coordinate with the private sector, including open-source communities and manufacturers, to improve the sharing of information.

Civil-military cooperation

The Blueprint identifies relevant interlocutors on the military side, highlighting the importance of civil-military cooperation in cyber crisis management, including but not limited to cooperation with NATO. The importance of cooperation with the military sector was stressed also in the 2025 'Warsaw Call' declaration, in which Member States identified civilian-military cooperation in the cyber domain as one of the key areas guiding EU's cybersecurity efforts[75].

The declaration outlined strategic areas for cooperation, such as situational awareness and crisis management, including EU-NATO cooperation – while respecting the principles of inclusiveness, reciprocity and the decision-making autonomy of both organizations. Furthermore, the EU cyber defence policy aims at enhancing cooperation and investments to better detect, deter, protect and defend against a growing number of cyberattacks. The 2025 Blueprint explicitly mentions EU military actors, such as the EU Cyber Commanders Conference[76] and the Military Computer Emergency Response Team Operational Network (MICNET)[77]. However, structured modes of cooperation with military counterparts to the EU's structures for civilian crisis management – such as the CSIRTs network or EU-CyCLONe – have not been defined yet.

3.2.2 Information sharing and situational awareness

A key component of an effective crisis management mechanism is the availability of consolidated EU-wide situational awareness that provides a clear overview of the threat landscape and the severity and impact of incidents. In recognition of this, the Blueprint requires MS and relevant Union entities to take necessary measures to enhance situational awareness, recognizing that the threat landscape and incident-specific situational awareness require distinct modes of operation[78].

At the EU-level, similarly to what was reported in 2024, work towards a comprehensive common, real-time picture encompassing all MS and covering all aspects of situational awareness has been ongoing.

Nevertheless, since 2024, empirical evidence shows an increase in trust and engagement among many of the parties that should create this picture. The EU Joint Cyber Assessment Reports[79] (EU-JCAR), foreseen by the CSA[80], describe the EU cyber threat landscape based on a combined understanding of a multitude of actors every quarter. Published as a joint product of ENISA, EUROPOL (EC3) and CERT-EU, these reports are based on open source and closed-source monitoring, with input from a volunteer group of MS. Insights are also received from a closed group of private sector companies within the framework of the ENISA Cyber Partnership Programme (CPP – *see Info box below)*.

75 Polish Presidency of the Council of the European Union, Warsaw Call Declaration adopted at the Informal TTE Telecom Council on Cybersecurity, available at: https://polish-presidency.consilium.europa.eu/en/news/warsaw-call-declaration-adopted-at-the-informal-tte-telecom-council-on-cybersecurity/ (accessed 9 June 2026).

76 'Cyber Commanders Conference' is an umbrella term that covers periodic 'conferences' (meetings) that gather cyber commanders at the rank of general from MS.

77 MICNET (Military Computer Emergency Response Team Network) is a voluntary network for technical cooperation among military CERTs.

78 European Council, *Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management*, available at: https://eur-lex.europa.eu/eli/C/2025/3445/oj (accessed 15 September 2026).

79 The Reports are only available to members of the CSIRTs Network and shareable with the national authorities of EU MS, EU institutions, IICB and the Council Horizontal Working Party on Cybersecurity Issues.

80 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 *Cybersecurity Act*, available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng (accessed 9 June 2026), Art. 7(6) he CSA states, *ENISA, in close cooperation with the Member States, shall prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats based on publicly available information, its own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2016/1148, both on a voluntary basis, EC3 and CERT-EU.*

Infobox: Cyber Partnership Programme (CPP)



Acknowledging the role of the private sector and seeking to increase trust between MS and private industry, ENISA has developed the Cyber Partnership Programme (CPP).

The Programme is designed to enhance information sharing and foster the cooperation necessary to strengthen the EU's cybersecurity landscape.

This is mainly done via:

- Voluntarily sharing of information on threats, incidents and vulnerabilities based on specific criteria set by ENISA;
- An open channel between the partners and ENISA to request information based on a specific ENISA interest (for example, support of EU-JCAR);
- ENISA acting as proxy to provide information on threats, vulnerabilities and incidents at the request of the CSIRTs Network, EU-CyCLONe and Union entities.

The effectiveness of information exchange depends significantly on the level of trust between the exchanging parties; nevertheless, national capacities to gather information as well as political, economic and technical constraints play a pronounced role too.

Information sharing from authorities in MS with the EU can be hampered by national legal frameworks or considerations juxtaposing the benefits of information sharing with national or operational interests. The likely under-reporting of significant incidents to the EU[81], for example, can be seen under this angle.

MS might also gather and deal with threat intelligence differently. The 2024 Report mentioned that all countries monitor their cybersecurity threat landscape, and have specific means (e.g. dedicated tools, reports) to do that. The picture has remained stable with improvements observed in the number of countries that produce and update threat landscapes periodically. Differences persist in the frequency of monitoring reports and in the way MS communicate with essential and important entities in case of need.

Concerning information exchange with the private sector, besides essential and important entities – treated in other parts of the current Report – **it is worth mentioning the constraints on the relationship between public authorities and specialised cybersecurity companies.** For some such companies, intelligence and visibility on the threat landscape are part of their core business and competitive advantage, and while a significant amount of pro-bono activity can take place, the business logic places a limit on the amount of free information sharing. Equally, for other companies, sharing information may expose sensitive operational data of the victims of incidents who may be their customers[82].

Also, from a technical perspective, gaps in tooling and interoperability persist, as different actors rely on different platforms and formats for exchanging data. A common taxonomy to ensure that all parties apply consistent terminology when reporting incidents is also lacking.

3.2.3 The importance of testing and getting ready: exercises.

To this day, the EU Blueprint for cyber crisis management has never been triggered by a real-world situation, but iterative testing through structured exercises has yielded valuable insights for its operational refinement. In November 2025, the new Blueprint was tested for the first time by cybersecurity crisis management executives across the EU and MS in the European Council, marking a major step forward in cooperation[83]. In June 2026, all the layers of the Blueprint (technical, operational and political) were fully tested during **Cyber Europe**[84], the largest pan-European exercise.

These simulations have provided critical evidence on the practicalities of the framework, highlighting both its strengths and the necessary adjustments required for a seamless implementation. This helps bridge the gap between theoretical policy and operational reality, with respect to the role of the operational layer in the new Blueprint.

81 2024 Report on the State of Cybersecurity in the Union

82 ENISA, 2025, *State of Cybersecurity in the Union – Panel Series: Revising the EU Cybersecurity Blueprint – Expert perspectives* (https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/state-of-cybersecurity-in-the-union-panel-series) (accessed 9 June 2026).

83 ENISA, BlueOLEx 2025: Testing the Capabilities of EU Crisis Management Executives, available at: https://www.enisa.europa.eu/news/blueolex-2025-testing-the-capabilities-of-eu-crisis-management-executives (accessed 9 June 2026).

84 ENISA, Cyber Europe 2026: All eyes on the EU's Collective Response and Resilience, available at https://www.enisa.europa.eu/news/cyber-europe-2026-all-eyes-on-the-eus-collective-response-and-resilience (accessed 4 July 2026).

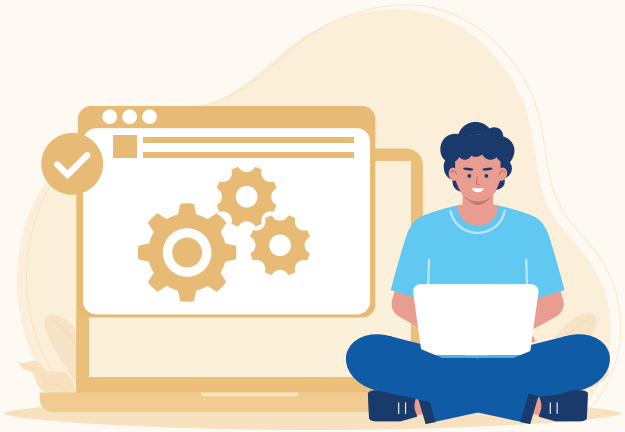
After having consulted EU-CyCLONe and the CSIRTs network, in July 2026 the EC, in coordination with the High Representative and supported by ENISA, compiled the first annual rolling programme of cyber exercises. This annual programme aims to prepare for cyber crises, enhance organisational efficiency, and account for exercises of the Union Civil Protection Mechanism (UCPM) and other EU-level crisis response mechanisms, including those outlined in the EU Critical Infrastructure Blueprint.

The 2024 Report stated that participation in EU-level exercises was high, while the organisation of structured national exercises appeared less consistent. This asymmetry between EU-level engagement and national capacity continues to represent a structural risk to EU-wide responses to crises. The lack in many cases of mechanisms in place to yield the benefits from operational learning amounts to a missed opportunity. There has been an increase in the number of countries with a coordinating body overseeing the organisation of exercises (from 16 to 19) and having an established cybersecurity exercise program at a national level (from 12 to 16), signalling an overall positive trajectory of institutional maturity across the EU. On the other hand, the number of countries having an established process to review, update and adapt the programme of exercises in order to incorporate lessons learned and the need for revised testing has decreased slightly (from 11 to 8). But the reason for this is not clear.

It is worth noting that interesting national approaches to cybersecurity exercises are emerging[85], such as the following.

- **Multi-Layered Testing**. A growing majority of observed exercises now test technical, operational and strategic skills all at once, showing a real leap in maturity of how these exercises are designed.
- **Private Sector Inclusion**. More advanced exercise programmes actively include the private sector. In 2024–2025, reported private sector participation was very high. Interestingly, the majority of exercises that engaged the private sector also featured international participation, suggesting that private sector openness and international openness tend to go hand in hand in more mature exercise cultures. This highlights the need for formalising private sector involvement through legislative frameworks, particularly for exercises targeting critical infrastructure.
- **Sector Diversification**. Exercises in the 2024–2025 cycle targeted multiple sectors, Energy, Digital Infrastructure, Public Administration, Healthcare and ICT. The healthcare sector appeared as a new exercise focus in 2025, with dedicated exercises taking advantage of the replicability of scenarios like those of Cyber Europe 2022 (which focused on health). This signals that MS are beginning to treat healthcare with the same exercise rigour historically reserved for energy and digital infrastructure. It also indicates that the targeted policy actions, like the Action Plan on the cybersecurity of hospitals and healthcare providers, can lead to diverse effects in increasing the maturity of the sectors.

Infobox: ENISA Cyber Exercise Methodology



In February 2026, ENISA published the ENISA Cyber Exercise Methodology[86], a comprehensive framework to help MS plan, design and structure cybersecurity exercises. The methodology addresses the full exercise lifecycle, from scoping and scenario design through to after-action review and integration of lessons identified.

This methodology responds to a major gap identified in previous years: the lack of a standardised, easy-to-use guide for MS.

85 These observations are based on the exercises in which ENISA has been involved as (co)-organisers, planners, observers etc. This also includes MS that had replayed a previous scenario by CyberEurope, financed by the Support Action Programme.

86 ENISA, The ENISA Cybersecurity Exercise Methodology, available at https://www.enisa.europa.eu/publications/the-enisa-cybersecurity-exercise-methodology (accessed 15 September 2026).

Policy Recommendations

The 2025 Blueprint provides a solid basis for more structured cooperation, especially among public civilian actors. Still, aspects related to the involvement and capacity of all relevant actors as well as information sharing need fine-tuning and improvement.



Key recommendations:

- **[MS and the EC]** should invest further in the maturity of the CSIRTs appointed to the CSIRTs Network and ensure that they proactively and fully use the CSIRTs Network Maturity Framework, including the related peer reviews, as part of their advancement process. They should mobilise efforts to raise their maturity to 'established' within the next two years.
- **[EU CyCLONe members, with the support of ENISA]** should clearly define the operational and crisis management role and responsibility of EU CyCLONe vis-à-vis the overall ecosystem, based on the experience gained since its formulation.
- **[ENISA in collaboration with other Union entities and the MS]** should build common situational awareness, based on a common taxonomy and shared data that is underpinned by validated joint analysis. Such situational awareness should also coherently integrate information from sources under different reporting frameworks, such as NIS2 and CRA.

Other recommendations:

- **[MS]** should further develop structured modes for interacting with the private sector and essential and important entities, to ensure that information sharing is timely and allows for the assessment of cross-border and supply-chain impacts.
- **[EU civilian crisis management actors]** should continue collaborating with their military counterparts to define structured modes for cooperation.
- **[The EC and ENISA]** should strengthen the value of information sharing beyond compliance by developing initiatives for the timely exchange of information about incidents moving towards a complete picture of situational awareness.
- **[MS]** should step-up to ensure that their participation in EU-level exercises matches their national targets for exercises and to codify formal processes to turn outcomes into real-world procedural updates.



ADVANCING THE **RESILIENCE OF CRITICAL INFRASTRUCTURE**

3.3 Advancing the resilience of critical infrastructure



Summary

Since the previous edition of this report, overall cybersecurity maturity across critical sectors seems to be steadily improving, along with an understanding of the specifics of the various sectors. Cybersecurity legislation and political attention have acted as drivers for investments.

Still, progress remains uneven both across and within sectors. Organisations consistently report facing challenges in attracting and retaining cybersecurity talent, although a few sectors are in a better position to compete for the limited talent pool available, e.g. through offering better working conditions or career development. At the same time, while NIS2 requirements are uniform for all essential and important entities, the operational realities of each sector are not uniform. Another layer of divergence emerges within the sectors themselves, particularly between large organisations and SMEs, which can be both more exposed and less prepared to deal with cyberattacks than their large counterparts.

Other factors are introducing additional considerations with regards to the resilience and preparedness of critical sectors. A sub-set of NIS2 essential entities will have to comply also with CER and take appropriate measures to ensure resilience in a broader sense. A defence dimension is also being introduced in the approach to critical infrastructure.

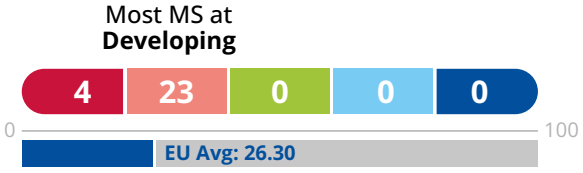
Finally, the speed and scale introduced by AI-enabled threats might translate into increased exposure of less prepared critical organisations, exacerbating existing differences.

Since the previous edition of this Report, cybersecurity maturity across critical sectors seems to be steadily improving as organisations respond to the evolving policy requirements and to the cyber threats they face. Several compounding factors are contributing to these improvements, including developments in cybersecurity legislation and increased political attention but also progress in the assessment of specific dimensions of maturity.

Be it sector-specific like DORA or horizontal like the NIS2 Directive, cybersecurity legislation has certainly contributed to this progress. For example, evidence suggests that both the Banking and Financial Market Infrastructures (FMIs) sectors have improved their cybersecurity maturity, also because the provisions in DORA are reinforcing collaboration and information sharing amongst FMIs, while strengthening supervisory authorities, which have further integrated cybersecurity into their activities[87].

At the same time, cybersecurity legislation has also acted as a key driver for cybersecurity investment[88]. Organisations surveyed across critical sectors are using it as a lever to secure resources to improve their cyber maturity in a more substantive way beyond legal compliance. Data show that, while 70% of organisations surveyed reported compliance as the main driver behind their cybersecurity investments[89], a substantial share had already realised that benefits extend well beyond compliance. These included better identification and mitigation of risks (41%), faster detection of incidents (35%), and improved incident response and recovery capabilities (26%). This is also evidenced by the NIS2 areas identified as most challenging by the organisations surveyed, namely vulnerability and patch management, business continuity and disaster recovery, and the management of supply-chain risk[90]. These are complex areas in the management of cybersecurity risk and go beyond superficial aspects. In fact, as regards the management of supply-chain risks, 90% of entities surveyed suggested they implement controls to better manage risks stemming from their supply chains[91]. Supply-chain risks were the second most cited concern by entities[92]. Finally, this increased focus on attaining meaningful outcomes while aligning with compliance obligations is also evidenced in the areas where entities intend to invest more going forward, namely strengthening effectiveness through tooling, enhancing resilience and increasing capacity and capability[93].

Greater political focus has also contributed to improvements in recorded maturity across certain sectors. Putting them in the spotlight reinforces the understanding that their cybersecurity must be improved, creating expectations around it and increasing awareness. Examples include the European Action Plan on the cybersecurity of hospitals and healthcare providers that has also led to the creation of guidance to inform changes to the cybersecurity policies, procedures and controls of entities[94] in the sector. Greater attention has been given also to sectors such as railway and maritime, for example under the Port Strategy[95], due to their increased role in military mobility, reflecting the need to strengthen the EU's resilience and strategic autonomy.



Participation by essential/important entities in information sharing activities

Observed improvements in maturity have also been driven by progress across specific dimensions of maturity, e.g. information sharing and collaboration. Evidence of this progress can be seen in the existence of structured mechanisms for collaboration among sectoral and national authorities under NIS2 and other sector-specific legislations[96]. It is also reflected in the more active engagement of organisations in sectoral ISACs and the expanding membership of EU ISACs[97]. Notwithstanding this progress, participation levels in non-mandatory information sharing amongst organisations in critical sectors can be further improved. This is corroborated by the relevant EU-CSI indicator tracking participation of essential and important entities in

87 ENISA, *NIS360*, 2026, available at: https://www.enisa.europa.eu/enisa-nis360-2026 (accessed 2 June 2026).

88 ENISA, *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 2 June 2026).

89 According to the ENISA *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 2 June 2026), 70% of organisations surveyed identified regulatory compliance with the requirements stemming from frameworks such as the NIS2 Directive, the CRA, or DORA, as the main driver of their cybersecurity investment over the past year.

90 According to the ENISA *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 2 June 2026), organisations surveyed identified the following three areas as the most challenging for them when it comes to aligning with NIS2 requirements: vulnerability and patch management (50%), business continuity and disaster recovery (49%) and supply-chain risk management (37%).

91 According to the ENISA *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 2 June 2026), these controls include: requiring suppliers to comply with security standards and maintain certifications (63%), conducting supplier risk assessments or audits (54%) and including cybersecurity requirements in supplier contracts (48%).

92 According to the ENISA *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 2 June 2026), the concern about supply chain attacks was cited by 47% of entities surveyed and was the second most cited after ransomware which was cited by 55% of entities.

93 According to the ENISA *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 2 June 2026), the most cited areas where organisations anticipate to focus their investments going forward were: upgrading cybersecurity tools (47%), improving resilience (34%), expanding training and awareness programmes (33%), and investing in cybersecurity staff (31%). Achieving or improving compliance with cybersecurity regulations was not a top priority, ranking sixth among the areas cited.

94 According to the ENISA, *NIS360*, 2026, available at: https://www.enisa.europa.eu/enisa-nis360-2026 (accessed 2 June 2026), in the health sector the majority of entities surveyed, indicated that in the past year they have made use of available guidance to inform changes to their cybersecurity policies, procedures or controls.

95 EU Port Strategy, available at: https://transport.ec.europa.eu/news-events/news/commission-unveils-eu-ports-strategy-strengthen-competitiveness-security-and-sustainability-european-2026-03-04_en (accessed 29 September 2026).

96 ENISA, *NIS360*, 2026, available at: https://www.enisa.europa.eu/enisa-nis360-2026 (accessed 2 June 2026).

97 ENISA, *NIS360*, 2026, available at: https://www.enisa.europa.eu/enisa-nis360-2026 (accessed 2 June 2026).

information sharing as part of at least one of a national ISAC, an EU-ISAC or an industry association. This is particularly relevant for sectors that are very diverse and operate across borders and/or across sectors or lack resources. Examples include sectors such as ICT Service Management, Cloud and Datacentre Services, Space, Public Administration, Drinking and Waste Water.

Despite maturity steadily improving across sectors, progress remains uneven both across and within sectors. Several factors contribute to these variations including skill shortages, sector-specific characteristics and different organisational sizes. Each of these factors is explored in more detail below.

- **Across sectors, organisations consistently report facing challenges in attracting and retaining cybersecurity talent**. This is partly the result of a structural constraint: the supply of cybersecurity professionals is simply not enough to meet the demand. According to the 2025 NIS Investments study, 45% of the organisations surveyed face difficulties in finding professionals having the required cybersecurity skills, with studies suggesting the cybersecurity workforce gap is indeed increasing (Section 3.5). That said, the challenge in attracting and retaining talent, can also be attributed to sectoral factors. Certain sectors (e.g. Banking) seem to be in a better position to offer competitive salaries, career development or better working conditions. Thus, such challenges have a lesser impact on them[98]. This points to a noteworthy dynamic: **the cybersecurity skills gap amplifies pre-existing disparities among sectors**, placing those who are in a better position to compete over the limited talent pool and secure the skills they need to deliver on their cybersecurity objectives.

- **While organisations across almost all sectors face similar challenges when it comes to aligning with the requirements of NIS2, the underlying causes of those challenges differ among sectors.** In some sectors and subsectors (e.g. Electricity, Gas, Railway, Drinking Water, Waste Water and Public Administration) legacy systems can be prevalent within their infrastructures and these are often no longer supported or are difficult or very expensive to patch or replace. Other sectors (e.g. Banking, Space and Health[99]) are challenged by complexities arising from operating across jurisdictions. Finally, certain sectors (e.g. Digital Infrastructure) identify a lack of skilled personnel or internal expertise as the key barrier preventing them from successfully aligning with NIS2 requirements[100]. **This highlights a key point: while NIS2 requirements are uniform for all essential and important entities, the operational realities of each sector make the feasibility and effort required to align with those requirements far from uniform across sectors.**

- **Yet another layer of divergence emerges within the sectors themselves, particularly between large organisations and SMEs.** SMEs surveyed in the context of the 2025 NIS Investments study consistently reported greater difficulty in competing with their larger counterparts in attracting and retaining cybersecurity talent[101]. They also reported greater challenges in aligning with NIS2 requirements and implementing foundational controls[102] as well as lower confidence in their ability to anticipate, withstand and recover from cyber incidents[103]. These challenges may in part be attributed to the more resourced-constrained nature of SMEs. They contribute to a reality where **certain small and medium-sized entities operating in highly critical sectors are both more exposed and less prepared to deal with cyberattacks** than their larger counterparts.

Other factors are also introducing additional considerations with regards to the resilience and preparedness of critical sectors. NIS2 promotes an all-hazards approach to managing risks against the security of networks and systems and their physical environment, which includes measures to protect such systems from system failures, human errors, malicious acts or natural phenomena[104]. It is complemented by the CER Directive for a more comprehensive view of resilience. The CER Directive follows an all-hazards approach, whether natural or man-made, accidental or intentional. By July 2026, MS had to identify critical entities within the scope of NIS2 and communicate them to the NIS2 authorities within one month of identification. Entities identified as critical entities under CER must comply also with NIS2. This means that **a sub-set of NIS2 essential entities will have to comply also with CER and take appropriate measures to ensure their resilience**, considering a variety of elements such as the reduction of disaster risk and measures to adapt to climate change as well as the identification of alternative supply chains.

---

98 ENISA *NIS Investments - Survey data companion document*, 2025, available at: https://www.enisa.europa.eu/sites/default/files/2025-12/NIS%20Investments%202025%20-%20Survey%20data%20companion%20document_0.pdf (accessed 3 June 2026) – section 3.12 Challenges to attracting cybersecurity talent (Sectoral view).

99 According to the ENISA *NIS Investments, 2025*, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 3 June 2026), in particular entities inside the Health sector that may operate across multiple MS, such as the manufacturing of pharmaceuticals.

100 ENISA *NIS Investments - Survey data companion document*, 2025, available at: https://www.enisa.europa.eu/sites/default/files/2025-12/NIS%20Investments%202025%20-%20Survey%20data%20companion%20document_0.pdf (accessed 3 June 2026) – section 3.18 Main obstacles to implementing NIS2 requirements (Sectoral view) – Corroborated by data gathered in the context of the latest ENISA, *NIS360*, 2026, available at: https://www.enisa.europa.eu/enisa-nis360-2026 (accessed 3 June 2026).

101 ENISA *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 3 June 2026), Insight#2 – SMEs box - 94% of SMEs report difficulties attracting and 90% retaining cybersecurity personnel (vs 83% and 80% among large enterprises).

102 The ENISA *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 3 June 2026), Insight#4 – SMEs box – Top reported barriers to effective implementation of NIS2 controls and Insight#5 – Comparison between Large and SMEs in terms of cybersecurity assessments conducted in the past year (Fig. 12) and average time to patch critical vulnerabilities on critical systems (Fig.15)

103 The ENISA *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 3 June 2026), Insight#7 – SMEs box – Perceived preparedness against specific scenarios SMEs vs large enterprises (Fig. 20).

104 NIS2 Directive (Directive (EU) 2022/2555), available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (accessed 3 June 2026). According to Recital 79, the aim of such measures would be to protect network and information systems and the physical environment of those from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access, damage or interference.

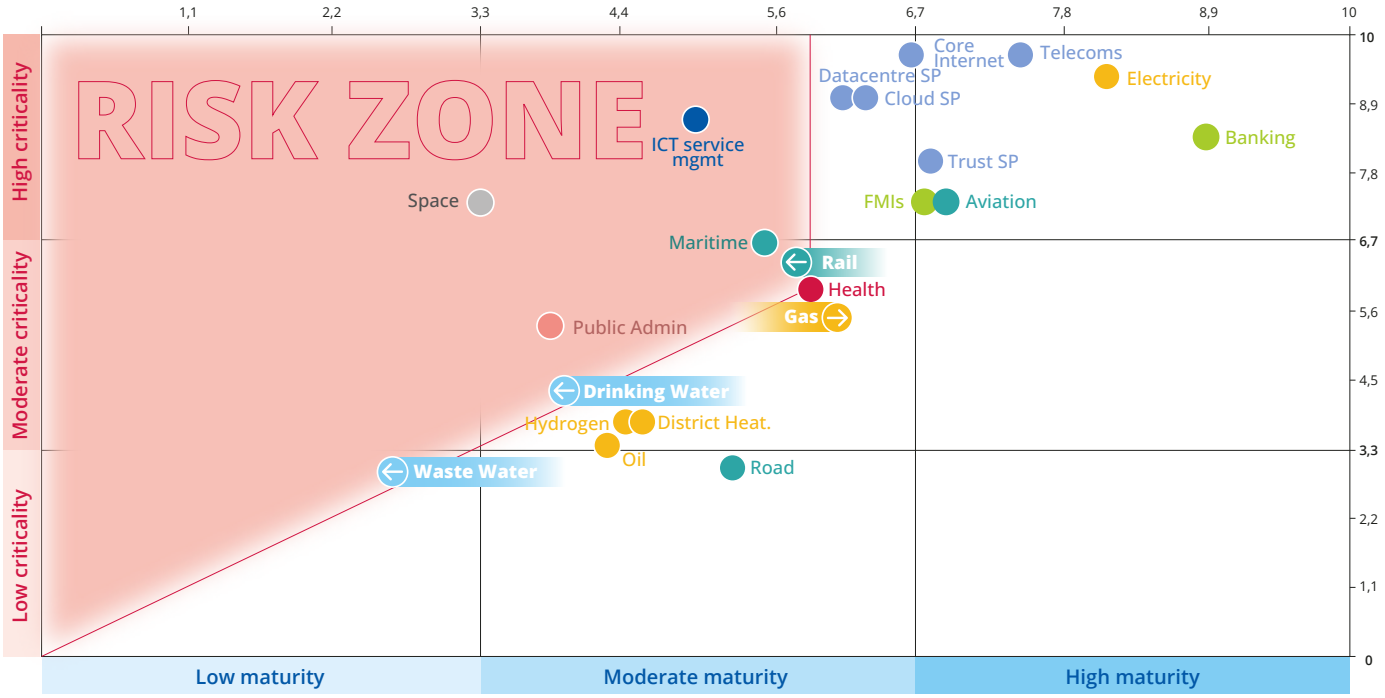
A defence dimension is also being introduced in the approach to critical infrastructure. For example, the 2025 Military Mobility Package covers the strengthening of the digital systems underpinning military mobility and ensuring the resilience of dual-use infrastructure. Also, based on the package, critical infrastructure that supports military mobility, including ports, airports, energy and communications nodes, will now be systematically identified and safeguarded[105].

Finally, **the speed and scale introduced by AI-enabled threats and AI-powered vulnerability discovery might translate into an increased exposure of critical organisations that are less prepared than others**. This may exacerbate existing differences. The immediate problem is the security of legacy products and in particular open-source components which form a critical part of the technology stack in use. There is also a risk that small organisations will not manage to obtain access to software or product testing capabilities enabled by new AI models due to costs[106]. At the same time, frontier AI models have proven capable of contributing to the cybersecurity posture of organisations. They can speed up the identification of cybersecurity weaknesses, assist in the development of mitigation measures and possibly improve the response time to threats.

3.3.1 EU-wide sector maturity

Building upon the recommendations of the 2024 Report on the State of Cybersecurity in the Union, ENISA further expanded and enhanced its studies to provide a comprehensive EU-wide overview of the cybersecurity maturity, preparedness, investment priorities and gaps in critical sectors. Using qualitative and quantitative indicators, the latest edition of the ENISA NIS360 study's methodology evaluates all sectors of high criticality[107], across three dimensions of criticality[108] and four of maturity[109], as depicted in the figure below. Annex B contains a sector-by-sector description of the maturity in the sectors

Figure 6: *EU-wide maturity and criticality of 22 NIS360 sectors and subsectors (2025)*[110]



105 European Commission, *Military Mobility Package*, 2025, available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/military-mobility_en (accessed 3 June 2026).

106 ENISA, ENISA's view on Cybersecurity in the Frontier AI Era, 2026, available at: https://www.enisa.europa.eu/publications/enisas-view-on-cybersecurity-in-the-frontier-ai-era (accessed 8 September 2026).

107 The methodology under the latest ENISA 360 study assesses all high criticality sectors as identified under NIS2 Annex I, presented in 22 (sub)sectors, as opposed to the 10 sectors introduced in the first edition of the State of Cybersecurity in the Union report.

108 Socio-Economic Impact of significant incidents, dependency on ICT to capture a sector's exposure and time criticality.

109 Policy framework and guidance, risk management and good practices, collaboration and information sharing and operational preparedness.

110 ENISA's NIS360 report analyses the NIS2 Digital Infrastructure sector by grouping its various entity types into subsectors, namely Core Internet Services, Telecoms, Cloud Services, Datacentre Services and Trust Services.

Policy Recommendations



The cybersecurity of critical infrastructure will increasingly depend on sectors developing their maturity according to their criticality and the effectiveness with which they can adopt broader resilience strategies. This includes overcoming legacy limitations, maintaining operational continuity, managing supply-chain risks, coping with the speed and scale introduced by AI-enabled threats, and dealing with increased geopolitical volatility.

Key recommendations:

- **[MS]** should require critical infrastructure operators to attest zero-trust baselines, resilient incident response capabilities during annual audits, and clear escalation paths for AI-accelerated incidents.
- **[MS]** should address the essential and important entities' needs in terms of cybersecurity skills and resources, using the ECSF to develop targeted capacity building activities and leveraging EU programmes to amplify efforts.

Other recommendations:

- **[ENISA]** should continue to facilitate the cooperation among NIS2 and CER authorities to ensure coherence in implementation and identification of overall critical dependencies at EU-level.
- **[MS and ENISA]** should support and/ or strengthen the participation of the private sector in sectorial information-sharing communities at the national and European level (ISACs). Sectors with low maturity should be prioritised.
- **[ENISA]** should facilitate cross-sector structured collaboration and coordination across different sectors, for example by leveraging on existing sectorial initiatives and ensuring coherence among them, focusing on sectors that have lower maturity but high criticality.



MANAGING **EU-LEVEL RISKS** AND **DEPENDENCIES** ACROSS SUPPLY-CHAINS AND BORDERS

3.4 Managing EU-level risks and dependencies across supply-chains and borders



Summary

The overall cybersecurity posture of a country is being increasingly determined by the cumulative level of security and trustworthiness of the goods and services on the market and their underlying components as well as of the entities making use of those goods and services.

The evolution of this topic in the last two years has been exponential, driven by the increased realisation of the real-world technical and strategic impact of dependencies within and across countries. Supply chain security, especially when cross-border, is a complex matter with implications extending beyond technical aspects. In the EU market, additional challenges may arise due to dependencies on foreign providers of technology, and exposure to strategic risks in specific sectors, underscoring the importance of tech sovereignty.

Several tools that have been designed to address the cybersecurity of supply chains. At the beginning of 2026, the NIS Cooperation Group adopted the EU ICT Supply Chain Security Toolbox[111]. This provides a common, non-legally binding framework for preparing and conducting EU-level coordinated security risk assessments of critical supply chains.

In addition, supply chain security elements embedded in EU legislation have started or continue to be implemented. In particular, vulnerability notifications are now more systematically reflected in cybersecurity legislation, including NIS2 and the Cyber Resilience Act (CRA). This is especially important as vulnerability exploitation remains a key vector for initial access and an increasing industrialisation of the discovery of vulnerabilities is being driven by frontier AI. Advances in EU legislation are accompanied by national efforts as vulnerability disclosure policies are becoming more embedded in national cybersecurity frameworks, although unevenly. Developments in the EU cybersecurity certification can also offer solutions, as reflected by the enlargement in the scope of certification to security services managed by third parties.

In addition, the EC proposed in January 2026, as a part of the revision of the Cybersecurity Act, the establishment of a trusted ICT supply chain framework to address non-technical risks related to the security the ICT supply chain.

All in all, the topic is only likely to grow in importance, underscoring the necessity for the EU and MS alike to further build capacity to handle complexity.

111 NIS Cooperation Group, EU ICT Supply Chain Security Toolbox, 2026, available at: https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security (accessed 9 June 2026).

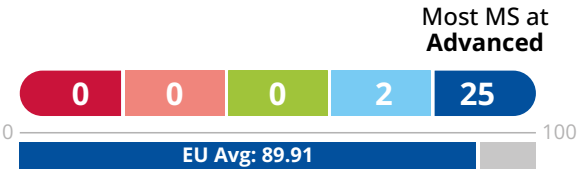
As anticipated in section 3.5, the variation in maturity observed both within and across sectors matters beyond individual organisations or sectors nowadays. Weaknesses in one entity can cascade to others through supply chains or service dependencies, regardless of the relative readiness or maturity of the sectors involved. In addition, the interconnection of world economies, combined with the impact of geopolitical and technological developments, means that **overall cybersecurity is being increasingly determined by the cumulative level of security and trustworthiness of the goods and services on the market, of their components and of the entities using them**.

Supply chain security, especially when cross-border, is a complex matter. Supply chain attacks and third-party compromises can be inherently difficult to detect and to mitigate. They can also be exacerbated by factors such as partial visibility and limited control over the practices of suppliers as well as location across borders and in other jurisdictions.

Implications extend beyond technical aspects. In the EU market, additional challenges may arise due to dependencies on foreign providers of technology and exposure to strategic risks in specific sectors. This can contribute to systemic dependencies within critical supply chains that are difficult to address and where organisations alone cannot reduce the exposure to risk. Still, market reality may make diversification or other mitigation measures particularly challenging. As highlighted in the Communication on European Tech Sovereignty[112], as geopolitical fragmentation deepens and supply chains are increasingly weaponised, excessive technological dependencies in critical sectors are becoming strategic liabilities.

Across the EU, organisations appear increasingly aware of these risks but feel generally unprepared. As anticipated in Section 3.3, the ENISA 2025 NIS Investments Study[113] shows that supply chain and third-party compromises rank as the second most frequently cited top concern (47%) among organisations surveyed. The overwhelming majority are already implementing mitigation measures. EU-CSI data show that, in the vast majority of countries, surveyed entities have measures in place to manage supply chain risk. Despite these efforts, over one-third of organisations (except in the banking sector) reported feeling predominantly unprepared, and 37% identified the management of supply-chain risks as the most difficult NIS2 requirement to implement.

At the same time, 43% of surveyed entities in the ICT service management sector conducted no cybersecurity assessments in 2024, and 45% took more than three months to apply critical patches to critical systems. Both figures point to a significant exposure to threats that timely identification of vulnerabilities and patching could have otherwise mitigated – with consequences extending beyond the sector itself to all entities that depend on those providers of ICT service management.



Supply chain management practices by essential/important entities

It is important to stress that outsourcing or buying goods and services from a third party should not be regarded as a weakness. For example, relying on external specialised expertise is a common practice to compensate for the lack of internal expertise and in line with the basic principle of transferring risks to entities that can professionally manage them. Still, the cybersecurity of a supply chain as a whole needs to be a priority and solutions can only be systemic and diverse.

The remainder of this chapter explores some of the tools that have been designed to address the cybersecurity of supply chains – and not only.

Good practices in Member States

Annual reporting of critical ICT and non-ICT suppliers gives the national competent authority visibility over shared dependencies across sectors. This can reveal suppliers whose disruption could have systematic consequences, including providers that do not themselves fall within the scope of the NIS2 Directive.

3.4.1 EU-level coordination and risk assessments

At the beginning of 2026, the NIS Cooperation Group adopted the EU ICT Supply Chain Security Toolbox[114], which provides a common, non-legally binding and structured approach for MS to identify, assess and mitigate the cybersecurity risks of ICT supply chains. Following an 'all-hazards approach', going beyond strictly technical aspects, it outlines risk scenarios encompassing both unintended and deliberate threats to ICT supply chains, as well as threats caused by external events (e.g. geopolitical tensions) and natural phenomena. The toolbox provides a general framework for preparing and conducting EU-level coordinated assessments of the security risks of critical supply chains based on Art. 22 of NIS2[115].

112 European Commission. Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy, 2026, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026DC0503 (accessed 10 June 2026).

113 ENISA, *NIS Investments*, 2025, available at: https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 2 June 2026).

114 NIS Cooperation Group, *EU ICT Supply Chain Security Toolbox, 2026, available at:* https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security (accessed 9 June 2026).

115 The Article provides that the NIS Cooperation Group, in cooperation with the European Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.

To give a sense of the breadth of the complexity of supply chain security *in practice*, the table below describes the main risks considered in the latest EU-level risk assessments, concluded in early 2026. Two additional risk assessments are being conducted, on Medical Devices and on Electricity Supply Systems and Energy Storage.

Connected and automated vehicles (2026)[116]. This risk assessment covers risks associated with several asset groups, such as processing and decision-making systems, vehicle control systems, communication and connectivity systems, sensing systems, charging infrastructure, cloud and backend systems, concluding with risks involving high-risk suppliers.

Detection equipment (2026)[117]. This risk assessment focuses on equipment that uses software and/or is interconnected to ICT systems used by EU law enforcement, customs and security operators for security screening and controls of goods and persons at ports, airports and other EU border crossings. It considers risk scenarios related to dependency or overdependency on a single manufacturer or a limited number of manufacturers, risks of intervention on the equipment due to equipment installation and maintenance, the introduction of malware, technical failures, unauthorised access to sensitive information, unauthorised monitoring etc.

These EU-level risk assessments are driven by volunteering MS, which pool and discuss information and assessments carried out at the national level, hence reflecting national specifics. The accuracy of EU-level risk assessments relies on national participation and national capabilities as well as cross-border consistency. This underscores the importance of building capacity and processes at national level to ensure that supply-chain risks are captured in their entirety and dealt systemically. The application of the measures proposed in the Toolbox need also to be handled at national level, as they remain purely recommendations.

3.4.2 Security-by-Design and vulnerability handling

As discussed in previous sections, the security of operations and also of supply chains starts from single components. Modern products are expected to be 'Secure-by-design' and 'Secure-by-default'[118]. Under the CRA, manufacturers of products with digital elements need to ensure that they meet essential cybersecurity requirements when they are being designed, developed, produced and deployed.

Still, threat actors continue to exploit both zero-day vulnerabilities and known vulnerabilities that remain unpatched. Widespread campaigns can now weaponise vulnerabilities within days, and in some cases even hours or minutes, of disclosure – while frontier AI will also bring down discovery time from days to hours[119].

For this reason, vulnerability handling is a key process to ensure that, when such vulnerabilities are discovered, they are timely and adequately assessed and contained. Effective disclosure and management of vulnerabilities help to reduce the window of exposure between vulnerability discovery, notification, remediation and, where appropriate, public disclosure.

Frontier AI and Vulnerability Handling[120]

In terms of frontier AI's impact on vulnerability management, vulnerability discovery is becoming increasingly industrialised. This lowers the marginal cost of identifying flaws and is likely to increase the volume, speed and complexity of vulnerability reports faster than many organisations can triage, validate and remediate them. ENISA's analysis of vulnerability disclosure notes that disclosure dynamics depend not only on technical discovery but also on incentives, coordination mechanisms and the costs borne by researchers, vendors, CSIRTs and defenders. In this context, rapid triage, prioritisation, coordinated disclosure and remediation are becoming more critical bottlenecks than discovery alone.

For example, to defend against lightning-fast automated cyberattacks, critical service providers may be forced to use autonomous patching as organisational approval is simply too slow. However, this creates a new risk in that automated updates could accidentally break systems and cause unwanted downtime. Furthermore, verifying these AI-generated patches may become a major bottleneck. System managers may face challenges in building tools that can quickly check and approve these fixes without accidentally introducing new bugs into the code. In this context, smaller organisations may find it more difficult to face the challenges than larger entities.

Where national CVD policies are in place and are supported by clear institutional responsibilities, trusted reporting channels and effective mechanisms for coordination they can enable earlier detection, orderly remediation and more consistent handling across sectors. Where such arrangements remain partial or underdeveloped, vulnerabilities may remain unreported, be handled inconsistently or be remediated too

116 NIS Cooperation Group, *EU Coordinated Risk Assessment on Connected and Automated Vehicles*, 30 January 2026, available at https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security NIS Cooperation Group, *EU Coordinated Risk Assessment on Connected and Automated Vehicles*, 30 January 2026, available at: https://www.ccam.eu/nis-cooperation-group-risk-assessment-on-connected-and-automated-vehicles/ (accessed 9 June 2026).

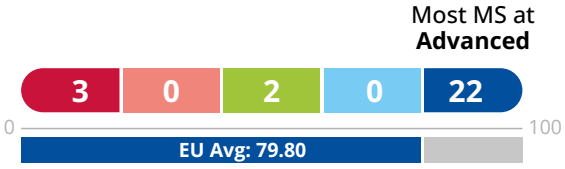
117 NIS Cooperation Group, *EU Coordinated Risk Assessment on Detection Equipment*, 30 January 2026, available at: https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security NIS Cooperation Group, *EU Coordinated Risk Assessment on Detection Equipment*, 30 January 2026, available at: NISCG_2026_Detection_Equipment_risk_assessment_WWJq0NuIChU7T4JRkFhgerhvcL4_124121.pdf (accessed 9 June 2026).

118 EENISA, *Secure by Design and Default Playbook*, 2026, available at: https://www.enisa.europa.eu/publications/enisa-secure-by-design-and-default-playbook (accessed 5 November 2026).

119 National Cyber Security Centre (NCSC) Netherlands, *Anthropic's frontier model Mythos calls for immediate action, available at:* https://www.ncsc.nl/nieuws/anthropics-frontiermodel-mythos-vraagt-om-directe-actie (accessed 9 June 2026).

120 ENISA, *ENISA's view on Cybersecurity in the Frontier AI Era,* 2026, available at: https://www.enisa.europa.eu/publications/enisas-view-on-cybersecurity-in-the-frontier-ai-era (accessed 8 September 2026).

slowly. This increases the risk of exploitation and contributes to fragmentation with potential negative effects on the overall cybersecurity posture across the EU.



Coverage of vulnerability disclosure policies

At the national level, Member States are making tangible progress in defining and implementing national CVD policies. Based on EU-CSI, with respect to 2024, the overall trajectory is positive, with a majority of MS having taken concrete steps, albeit at differing levels of maturity and operationalisation. Still, due to the prominent role AI plays in the exploitation and mitigation of vulnerabilities, the newly adopted EU Action Plan on Cybersecurity and AI invites the MS to reflect and update their CVD policies and timings.

Overall, the results suggest that vulnerability disclosure policies are becoming more embedded in national cybersecurity frameworks. Since 2024, the share of countries declaring not to have a national CVD policy yet (or to still be in the process of defining one) decreased from 17 to 7. When it comes to entities under NIS2, in the great majority of MS CVD policies apply across all 'high criticality' as well as 'other critical' sectors. This overall result suggests broad formal alignment with the sectoral scope introduced by NIS2, including for newer critical sectors. At the same time, a gap remains between formal policy definition and full operational maturity. The findings point to a transition phase in which CVD policies are being actively implemented only in some countries (15). Although this represents some progress compared to the situation in 2024 (10 MS)[121] the posture of MS with regards to CVD implementation is varied. This is resulting in less consistent implementation across the EU compared to the broader uptake of CVD policy.

Good practices in Member States

Proactively notifying website and device owners of known vulnerabilities, combined with regular publication of threat and vulnerability information, helps organisations remediate weaknesses before they are exploited. Lessons from incidents can thus be translated into practical preventive measures for both public- and private-sector organisations.

At the EU-level, vulnerability notifications are now more systematically reflected in cybersecurity legislation, including NIS2 and the CRA. In this context, ENISA is scaling its EU Vulnerability Services to better support MS, national CSIRTs, competent authorities, and the EU internal market. In accordance with NIS2, ENISA has already developed and maintains the European Vulnerability Database (EUVD)[122], which stores, enriches and publishes information about publicly disclosed vulnerabilities to help translate vulnerability identifiers into more actionable information about risk. The EUVD integrates Common Vulnerabilities and Exposures (CVE)[123] data, information provided by the CSIRTs Network, ICT vendors disclosing vulnerability information via advisories, and relevant information about known exploitations and the likelihood of exploitation, including sources such as known exploited vulnerability catalogues and the Exploit Prediction Scoring System (EPSS). By aggregating, enriching, correlating and operationalising this information, the EUVD contributes to a more timely, reliable and actionable vulnerability information ecosystem for the EU.

To better support CVD processes within national competences, ENISA has also reinforced its role in the global vulnerability management ecosystem, including through the CVE Program. ENISA has been providing CVE Numbering Authority (CNA) services since January 2024 and has been serving as the CVE Root for European entities since November 2025. Through this role, ENISA supports European CNAs, including national CSIRTs enrolled in the CVE Program. It does so by facilitating onboarding and training, strengthening coordination, supporting implementation of CVE Program requirements, and helping to improve the quality, completeness, machine-readability, accuracy and timeliness of vulnerability information. This role complements national CVD policies and processes by helping ensure that vulnerabilities coordinated through national or EU-level channels can be assigned, documented, published and referenced in a consistent and interoperable manner.

121 The ENISA interactive map on National Cybersecurity Strategies includes a section where MS have made available information about the implementation of national CVD policies: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/national-implementation/cvd-policy (accessed 9 June 2026).

122 ENISA, European vulnerability database, available at: https://euvd.enisa.europa.eu/about (accessed 9 June 2026).

123 A CVE ID (Common Vulnerabilities and Exposures Identifier) is a unique, standardised string assigned to publicly known cybersecurity vulnerabilities in software or hardware. These IDs serve as a universal language for the cybersecurity community, allowing vendors, researchers, and tools to track, prioritise, and fix specific security flaws without confusion.

At the level of products, the CRA introduces essential requirements for vulnerability handling for the products within its scope and mandates vulnerability management throughout the product lifecycle or support period. It also foresees vulnerability reporting obligations for actively exploited vulnerabilities through a dedicated platform, the CRA Single Reporting Platform (CRA SRP)[124]. From September 2026 onwards, manufacturers of products with digital elements have to report actively exploited vulnerabilities and severe incidents affecting their products through the platform. The platform can also be used by any natural or legal person to voluntarily report other vulnerabilities.

The CRA SRP is important because it creates a structured reporting channel and it also provides the EU with authoritative information on vulnerabilities and incidents directly from manufacturers. This should improve the EU's ability to prioritise, coordinate and support defensive actions based on timely and trusted information from the source. It also supports a *report once, distribute to many* logic, allowing relevant MS to receive information through a common mechanism and reducing the risk of information asymmetry.

To ensure overall coherence, the CRA also ensures that, after a security update or where another form of corrective or mitigating measure is available, notified vulnerabilities are made available on the EUVD with the agreement of the manufacturer. The structured reporting under the CRA SRP, combined with the additional vulnerability information provided in the EUVD, will enable reported information to be transformed, where appropriate, into actionable knowledge for defenders, operators, competent authorities and the wider EU market.

As vulnerability handling becomes increasingly more established across the EU, the main challenge is no longer initial policy uptake but achieving greater operational maturity, stronger convergence of national approaches, and more consistent implementation across the full vulnerability management lifecycle. Adoption, consistent implementation and full operationalisation of national CVD policies are foundational. Otherwise, disparities across MS may continue to create asymmetries in vulnerability intake, coordination, remediation and disclosure with implications for the overall level of cybersecurity across the EU.

Industry should also play an important role, with clear responsibilities and accountability, within the broader ecosystem and in close coordination with national and EU competent authorities. Manufacturers, vendors and other relevant operators must build and deploy better engineered products, systems and services by applying Secure-by-Design and Secure-by-Default principles across the product lifecycle; effectively implement vulnerability handling policies and CVD processes; and adopt all necessary measures to promptly identify, assess, mitigate, and remediate vulnerabilities, including by patching vulnerable systems once vulnerabilities are discovered. This is of the utmost importance in an era where frontier AI is compressing vulnerability discovery, triage, exploitation and remediation timelines, forcing competent authorities and industries across the globe to fundamentally rethink the vulnerability management lifecycle.

3.4.3 EU Cybersecurity certification

Introduced in 2019 with the Cybersecurity Act, the EU cybersecurity certification framework established harmonised cybersecurity requirements and methodologies to evaluate them across national markets and sectors for ICT products, process and services. Amended in 2025, the scope of the European cybersecurity certification framework was enlarged to cover security services managed by third parties ('managed security services'[125]). The framework enables manufacturers and providers to access national markets more easily and gives consumers a clearer understanding of the level of security in the solutions they purchase.

The development of European cybersecurity certification schemes is led by ENISA upon a request from the EC in accordance with the priorities set out in the Union Rolling Work Programme[126]. The EU cybersecurity certification scheme on Common Criteria (EUCC), the first one to be adopted[127], focuses on ICT products such as hardware and software products and components. It builds on the long existing SOG-IS certification framework. Other schemes are under development and will cover cloud services (EUCS)[128], 5G networks (EU5G), EU Digital Identity Wallets (EUDIW)[129] and managed security services (EUMSS)[130].

124 ENISA, CRA Single Reporting Platform, available at: https://portal.cra-srp.enisa.europa.eu (accessed 15 September 2026)

125 NIS2 defines a managed security service provider' as a 'managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management'.

126 ENISA, 2024, *Union Rolling Work Programme*, available at: https://certification.enisa.europa.eu/about-eu-cyber-certification/eu-regulatory-context/union-rolling-work-programme_en (accessed 9 June 2026).

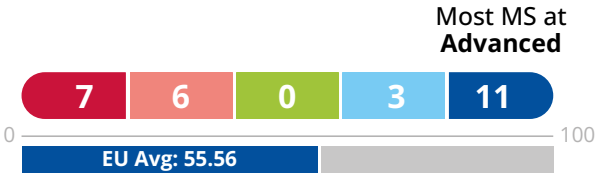
127 ENISA, 2025, *EU Cybersecurity Certification Scheme on Common Criteria (EUCC)*, available at: https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en (accessed 9 June 2026).

128 ENISA, *Consultation on the draft of the candidate Certification Scheme on Cloud Services (EUCS)*, available at: https://www.enisa.europa.eu/topics/consultation-on-the-draft-of-the-candidate-certification-scheme-on-cloud-services-eucs-closed (accessed on 03/06/2026).

129 ENISA, EUDI Wallet Certification Scheme, available at: https://certification.enisa.europa.eu/browse-topic/eudi-wallet_en (accessed 15 September 2026).

130 ENISA, EU Cybersecurity certification for Managed Security Services, available at: https://certification.enisa.europa.eu/browse-topic/eumss_en (accessed 15 September 2026).

EU certification schemes rely on the development of national ecosystems. Simplifying, these ecosystems are composed of National Cybersecurity Certification Authorities (NCCAs) that supervise, certify and monitor EU cybersecurity certification at national level, and Conformity Assessment Bodies (CABs) that can act as evaluators or certifiers. In the context of EUCC, IT Security Evaluation Facilities (ITSEFs) are also part of the ecosystem as they are technical laboratories performing security evaluations of ICT products.



National certification capabilities

Based on 2026 EU-CSI data, national certification capabilities for national and EUCC schemes show a clear split between countries in terms of the availability of national certification schemes, of certification bodies accredited (or in the process of being accredited) to deliver EUCC certificates, as well as of evaluation facilities accredited (or in the process of being accredited) to perform assessments under EUCC.

Given the relatively recent adoption of EUCC, it is normal that the maturity of MS on this matter is not homogenous. Countries that were already active with national schemes and that are qualified/authorising participants in the SOG-IS scheme are naturally more likely to have conformity assessment capabilities, even if new actors have emerged as well[131]. This imbalance is mitigated by the possibility that manufacturers of products could obtain certificates that are valid across the whole EU.

Still, uneven maturity could result in structural constraints that limit scalability and the uptake of EU cybersecurity certification as more schemes become available. For example, for managed security services, it is reasonably expected that certification markets will develop more locally, as the choice of service providers is often driven by trust, language and proximity. In addition, the EU can adopt a delegated act setting how a specific EU scheme can be used for presumption of conformity with the cybersecurity requirements of the CRA (Art. 27 CRA). Work is being conducted to guide the potential use of EUCC to this aim[132], which might further drive the demand for EU certification.

131 Based on 2026 EU-CSI, out of the 16 MS that have at least one national scheme established for cybersecurity certification for ICT products, processes or services, 12 MS have a Certification Body accredited to deliver certificates under EUCC (or are in the process of accrediting one). All countries that are qualified/authorising participants in SOG-IS also have a Certification Body accredited to deliver certificates under EUCC (or are in the process of accrediting one).

132 ENISA, 2025, *Cyber Resilience Act implementation via EUCC and its applicable technical elements, available at:* https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en (accessed 9 June 2026).

Policy Recommendations



Ensuring a consistently high-level of security and reliability across borders and in the current geopolitical landscape is becoming increasingly complex. Cybersecurity should be coherently integrated at every step of the value and supply chain, from secure development to secure operations.

Key recommendations:

- **[MS]** should build national capacity to contribute to EU-level risk assessments, building on the EU ICT Supply Chain Security Toolbox to ensure harmonisation and better and more reliable EU-level risk-assessments.
- **[The EC]** should ensure that the existing legal frameworks, including NIS2, CRA and the EU AI Act are leveraged, to make use of the benefits and tackle the cybersecurity risks stemming from AI, including the most advanced AI models.

Other recommendations:

- **[MS]** should prioritise investments in the implementation of measures for supply chain security in essential and important entities.
- **[MS with ENISA support]** should continue strengthening the adoption, consistent implementation, and operational maturity of national CVD policies.
- **[MS and ENISA]** should invest in and reinforce the interoperability of vulnerability services, platforms, and databases, including the EUVD, the EU KEV Catalogue, CRA SRP, national vulnerability coordination mechanisms, and relevant global systems such as the CVE Programme.


BUILDING
LONG-TERM
SOCIETAL
RESILIENCE,
AWARENESS,
SKILLS AND
EDUCATION

3.5 Building long-term societal resilience, awareness, skills and education



Summary

Despite some increase in digital skills, gaps in cybersecurity awareness persist and continue to affect a significant share of the population, suggesting that current approaches may not suffice, at least in the short term.

The integration of cybersecurity into national educational curricula at the primary and secondary levels remains limited and uneven. This is weakening resilience among future generations.

The cybersecurity skills gap has increased, with a perceived shift from staff to skills shortage. On the demand side, the gap is driven by the inability to find candidates as well as budget constraints. On the supply side, despite measures promoting cybersecurity in higher levels of education, the increase in graduates has slowed down. While investments are key, diverse approaches such as skills attestation, competitions and bootcamps, seem to be promising ways to address the skills shortage. Skills attestations can enhance the comparability of professional competences, while competitions and bootcamps can raise awareness of cybersecurity careers and create new pathways into cybersecurity professions.

Finally, AI is significantly reshaping the nature of the cybersecurity profession. On the one hand it is reducing roles requiring repetitive analysis, on the other hand demand is growing for expert positions that combine cybersecurity expertise with AI fluency.

Work on research and innovation in cybersecurity is driven by academia and final solutions have difficulties reaching the market. Topics are driven by technological developments as well as the geopolitical and regulatory context.

Awareness, education and professional skills development are fundamental for cybersecurity resilience. This is supported by the fact that social engineering remains a common enabling tactic to abuse trust, particularly through phishing campaigns[133]. Strengthening cybersecurity awareness among citizens, integrating cybersecurity into educational systems, and ensuring the availability of qualified cybersecurity professionals reduce cyber risks, support the secure digital transformation of society and enhance the EU's overall cybersecurity preparedness and competitiveness.

3.5.1 Cybersecurity Awareness and Education

Gaps in both digital skills and cybersecurity awareness persist and continue to affect a significant share of the population. This limits an inclusive uptake of digital services and reinforces existing inequalities in access to opportunities and exposure to cyber risks.

The Digital Decade programme sets a target of **at least 80% of adults possessing basic digital skills by 2030[134]. Approximately 60% of Europeans possess these skills**, after an encouraging increase of about 5% percentage points between 2023 and 2025[135].

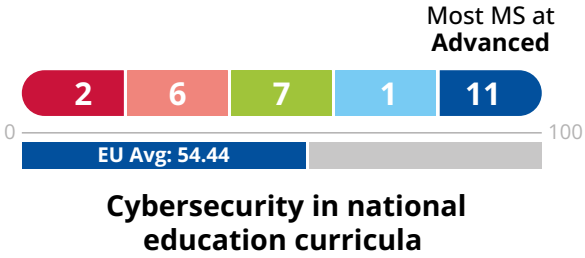
In parallel, evidence points to persistent **low levels of privacy awareness among EU citizens**. While some improvements can be observed, such as a rise in individuals restricting access to social media profiles (from 37% in 2023 to 43% in 2025)[136], the related metrics remain modest. Notably, only one in three EU citizens reports reading privacy policy statements before providing personal data, a figure that increased only slightly over the past years[137].

At the policy level, most Member States have formally recognised the importance of cybersecurity awareness and cyber hygiene, but not all of them have translated this into action. Based on EU-CSI, most MS have defined strategic objectives related to awareness-raising and the promotion of good cyber hygiene practices. However not all of them have fully implemented their action plan nor are they constantly monitoring actions in an effort to improve them. This gap in implementation highlights the need for stronger collaboration between public and private stakeholders (from both the demand and supply sides) as well as clearer ownership of initiatives in cybersecurity awareness.

Good practices in Member States

National campaigns, practical guidance and timely public threat notifications strengthen cyber risk awareness and promote protective behaviours. Combined with technical measures and incident preparedness, these measures translate awareness into practical cybersecurity resilience across society.

In the field of education, the integration of cybersecurity into national educational curricula at the primary and secondary levels remains limited and uneven across MS.



Cybersecurity in national education curricula

Based on the EU-CSI, roughly half of MS have embedded cybersecurity elements into primary (14 MS) and secondary (13 MS) school curricula, with little increase over the past two years. Notably, secondary school coverage has declined – from 17 to 13 MS – signalling a regression that warrants attention. This indicator is one of the least aligned, meaning that MS are very fragmented. This might be due to differences in educational systems, which, in most countries, are not centralised. The findings suggest that cybersecurity education is not yet systematically embedded in school systems across the EU, as the mandate for cybersecurity in education can be split between authorities. While this might reflect limitations in data collection[138], strengthening and harmonising the integration of cybersecurity education from an early age would help build a common baseline of digital resilience, cyber hygiene and safe online behaviour among future generations. When it comes to higher education, the EU-CSI measures the actions taken to include, promote and enhance cybersecurity in higher levels of education. There is still some dispersion, but overall, most MS have implemented a substantial share of the relevant measures. Evidence shows a stable, slightly increasing, picture from 2024.

133 ENISA, *ENISA Threat Landscape 2026*, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026 (accessed 22 September).

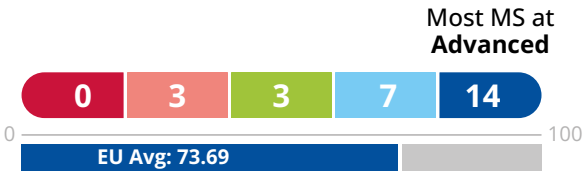
134 European Commission, 2025, *Europe's Digital Decade, Policy programme*, available at: https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme (accessed 9 June 2026).

135 Eurostat, *Individual levels of digital skills*, available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21/bookmark/line?bookmarkId=87a83924-0232-4c50-9b22-3a0a701ce32e (accessed 9 June 2026). It is to be noted that the increase from 2021 to 2023 was of only about 2.5%.

136 Eurostat, *Individuals that limited access to profile content on social networking sites or shared online storage*, available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_prv20/bookmark/table?bookmarkId=d2c52b34-d1f8-4083-a0f3-8b109385bc2d (accessed 9 June 2026).

137 Eurostat, *Individuals that read privacy policy statements before providing personal data*, available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_prv20/bookmark/table?bookmarkId=37e9f67d-8120-43e5-a0ac-2f79b39d68e6 (accessed 9 June 2026).

138 ENISA, EU Cybersecurity Index (EU-CSI) dataset (partially sourced from Member States, coverage varies depending on national educational systems, not fully harmonised across countries).



Cybersecurity in higher education curricula

For example, funding mechanisms to encourage the uptake of cybersecurity degrees have remained stable, with approximately two thirds of MS either establishing or actively implementing such schemes.

However, these efforts have yet to result in a significant impact. The number of cybersecurity graduates reported by the ENISA Cybersecurity Higher Education Database[139], although there was a steady increase over the past five years, has slowed during the last two years, potentially constraining the pipeline of future talent.

Good practices in Member States

An integrated approach to cybersecurity capacity building combines a national framework for skills, structured training programmes and regional competence centres. This enables the identification of skills gaps, the provision of targeted training and practical support for organisations – particularly SMEs and public administrations – to strengthen their cybersecurity maturity and resilience.

3.5.2 Cybersecurity skills

As reported in section 3.3, **organisations report facing challenges in attracting and retaining talent, although some sectors seem to be in a better position than others**. EU regulatory frameworks seem to have had an impact, to some extent, on the demand and qualification requirements for cybersecurity roles, as 1 out of 5 entities report the skills gap to be the main barrier to the implementation of NIS2 controls[140]. This means that the skills gap can also hinder regulatory compliance. Data also shows that NIS2 and DORA are reshaping hiring practices[141].

The World Economic Forum's Global cybersecurity Outlook 2025[142] shows **that the cyber skills gap has increased by 8% since 2024, with 'two out of three organisations reporting moderate-to-critical skills gaps, including a lack of essential talent and skills to meet their security requirements'**. Only 14% of organisations are confident that they have 'the people and skills they need today'. The downstream effects of the skills shortages are felt across the entire cybersecurity function. Organisations report delayed projects, slower incident response, reduced monitoring coverage and rising burnout among existing staff. In addition, a significant number of organisations link the lack of appropriate skills directly to security breaches[143].

On the demand side, skills shortages seem to be driven primarily by the inability to find candidates with the required skills and by budget constraints[144]. A shift in the views of organisations has been noted. Until recently, the shortage of qualified people in this field was regarded as the most prominent factor impacting the ability of organisations to effectively defend themselves. However, this view seems to have changed and the need for critical skills has been flagged as a more relevant than the need for more people[145] [146]. This underlines the need for stronger mechanisms for public-private cooperation that enable education and training systems to respond more rapidly to emerging industry requirements.

Addressing the skills gap over the medium and long term requires a sustained investment in the supply of qualified cybersecurity professionals for which public support is necessary. Higher education plays a large role in this as around one in three young individuals in the EU enter the cybersecurity field through higher education programmes in cybersecurity, while approximately one in two transition from IT roles[147]. Both routes are valuable. **However as seen above neither seems to grow fast enough to meet current demand**[148].

In this context, consistent monitoring of the cybersecurity skills gap and workforce needs is essential to support informed policy and investment decisions, and to better align education, training, and initiatives for the development of the workforce in line with market demand – an area where a coordinated and systematic approach has not yet been fully implemented across the EU.

A diverse mechanism for encouraging young people to

139 ENISA, *CyberHEAD – Cybersecurity Higher Education Database*, available at: https://www.enisa.europa.eu/tools/cyberhead-cybersecurity-higher-education-database (accessed 9 June 2026). The data featured in the database is based on voluntary data collection.

140 ENISA, *NIS Investments 2025, available at:* https://www.enisa.europa.eu/publications/nis-investments-2025 (accessed 9 June 2026).

141 SANS Institute, *2026 Cybersecurity Workforce Research Report*, available at: https://www.sans.org/mlp/2026-evolving-cybersecurity-workforce-ai-compliance-talent (accessed 9 June 2026).

142 World Economic Forum, *Global Cybersecurity Outlook 2025*, available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (accessed 9 June 2026).

143 SANS Institute, *2026 Cybersecurity Workforce Research Report*, available at: https://www.sans.org/mlp/2026-evolving-cybersecurity-workforce-ai-compliance-talent (accessed 9 June 2026).

144 (ISC)², *2025 Cybersecurity Workforce Study,* available at: https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study (accessed 9 June 2026).

145 (ISC)², *2025 Cybersecurity Workforce Study,* available at: https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study (accessed 9 June 2026).

146 SANS Institute, *2026 Cybersecurity Workforce Research Report,* available at: https://www.sans.org/mlp/2026-evolving-cybersecurity-workforce-ai-compliance-talent (accessed 9 June 2026).

147 (ISC)², EU subset of the *2025 Cybersecurity Workforce Study* (data provided to ENISA, not publicly available).

148 European Commission, *Digital Decade – ICT specialists indicator (DD-ICTSPEC)*, available at: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/dd-trajectories/charts/dd-trajectories-2025?breakdownGroup=digital_decade_2025&indicator=dd_ictspec&country=EU&unit=mio_ind (accessed 9 June 2026).

pursue careers in the field and develop hands-on skills is offered by competitions, bootcamps and challenges. For example, Capture-the-Flag competitions and Hackathons in general have been proven to be effective mechanisms to raise awareness of cybersecurity careers, develop practical professional skills among young individuals, including good teamwork, and create new pathways into the profession[149].

Building on the EU Cybersecurity Skills Academy, another mechanism is the proposed establishment of EU-wide cybersecurity **skills attestation schemes**[150] **through an EU framework implemented at national level**. This approach has been piloted recently, and findings suggest that it can help enhance transparency and comparability of professional competences across the EU as well support cross-border deployment of cybersecurity experts during incidents and operations. The CSA2 proposal provides for the European individual cybersecurity skills attestation mechanism.

3.5.2.1 The impact of AI on cybersecurity skills and the workforce

Technological advances in Artificial intelligence (AI) are significantly reshaping the nature of the work within cybersecurity teams. An ENISA study on Cyber skills[151] has indicated that AI is advancing in cybersecurity operations. AI enables the automation of workflows and reporting, leading to a fundamental shift on how cybersecurity tasks are performed. AI in cybersecurity spans multiple functions, supporting activities across the entire security lifecycle – from identifying risks and protecting systems to detecting threats, responding to incidents and enabling recovery[152]. For example, AI reduces the manual burden on SOC analysts – but simultaneously raises the bar for the skills required to operate and oversee these systems effectively. Cybersecurity defenders are integrating AI tools into cybersecurity operations, increasing the need for experienced cybersecurity professionals. Globally, organisations are beginning to reduce headcount in roles where repetitive analysis and pattern recognition constitute the bulk of the workload. At the same time, the introduction of AI systems adds a new category of AI risks which requires new personnel with additional specific AI skills. **Demand is growing sharply for expert positions that combine deep cybersecurity knowledge with AI fluency**. AI/ML security has emerged as one of the fastest-growing specialist domain. Professionals already identify it as the single most in-demand skill, while many hiring managers are still catching up[153]. This rapid structural shift in cybersecurity roles and skills underscores the need for systematic monitoring of AI-driven changes in the profession.

3.5.3 Research and Innovation in the EU (in collaboration with ECCC)

Infobox: The Role of ECCC

The European Cybersecurity Competence Centre (ECCC), together with the Network of National Coordination Centres (NCCs), support innovation and industrial policy in cybersecurity.
They jointly make strategic investment decisions and pool resources from the EU, MS and, indirectly, the industry to improve and strengthen technological and industrial cybersecurity capacities, enhancing the strategic autonomy of the EU. The Centre plays a key role in delivering on the ambitious cybersecurity objectives of the Digital Europe and Horizon Europe programmes.

In the EU, cybersecurity remains a specialised area driven by academia within broader research efforts. Publications related to cybersecurity represent a small fraction of the EU's total scientific output while the majority are produced by universities[154].

Signals from the cybersecurity market are also consistent with this pattern, underscoring the gap between research and market and the time required to translate the results of research into market-ready solutions. This is evident both in the small number of relevant EU patents in the ICT domain[155] and the fact that entrepreneurial support structures (such as accelerators and incubators) are not necessarily dedicated to cybersecurity alone.

The continued relevance of relatively recent R&I cybersecurity areas is being confirmed (for example, Artificial Intelligence (AI) and Post-Quantum Cryptography (PQC)), **while new topics emerge, also driven by the geopolitical context**. For example, the 2025 European Internal Security Strategy (ProtectEU Internal Security Strategy[156]) stresses the role of R&I in creating solutions to counter emerging threats, including from technology misuse, as well the potential dual-use of technologies to be exploited from civil to defence, and from defence to civil.

149 ENISA, data from European Cybersecurity Challenge survey (internal/ non-public dataset).

150 European Commission, *Cybersecurity Skills Academy – proposal for ENISA pilot on attestation of cybersecurity skills*, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_26_105 (accessed 9 June 2026).

151 ENISA study not publicly available.

152 World Economic Forum, 2026, *Empowering Defenders: AI for Cybersecurity (2026),* available at: https://reports.weforum.org/docs/WEF_Empowering_Defenders_AI_for_Cybersecurity_2026.pdf (accessed 9 June 2026).

153 SANS Institute, 2026, *2026 Evolving Cybersecurity Workforce: AI, Compliance & Talent,* available at: https://www.sans.org/mlp/2026-evolving-cybersecurity-workforce-ai-compliance-talent (accessed 9 June 2026).

154 ENISA, internal data (non-public source).

155 Centre on Regulation in Europe (CERRE), 2025, *Competitiveness, Digital Transformation and EU Policies Issue Paper,* available at: https://cerre.eu/wp-content/uploads/2025/11/CERRE_Competitiveness-Digital-Transformation-and-EU-Policies_Final.pdf (accessed 9 June 2026).

156 European Commission, *Communication from the Commission on ProtectEU: a European Internal Security Strategy, COM(2025) 148 final,* available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0148 (accessed 9 June 2026).

At the same time, new regulatory areas and the legislative framework call for public authorities and private companies alike to strengthen their capacity and acquire capabilities, at times in new domains. This results in an increased need to explore and deploy innovative solutions, backed by adequate resources.

These continuously evolving needs stress the importance of a flexible approach when defining research and innovation (R&I) priorities.

3.5.3.1 Strategic areas for EU R&I investment

The EU has committed EUR 1.4 billion on cybersecurity funding in the period 2021-2027 through two main funding instruments. **Horizon Europe** supports the research and development of technology and innovation. The **Digital Europe Programme** is dedicated to the deployment and uptake of cybersecurity technologies. Together, these programmes create a European cybersecurity innovation pipeline, linking research and technological development with deployment and operational uptake. This approach is intended to accelerate the transition from research results to market-ready solutions, while supporting the broader policy objectives of resilience, competitiveness and digital sovereignty.

Figure 7: *Examples of R&I pipelines.*

THEMATIC AREA	HORIZON EUROPE PROGRAMME Research and innovation	DIGITAL EUROPE PROGRAMME Deployment and uptake
AI FOR CYBERSECURITY	Development of trustworthy AI for cybersecurity applications, such as threat detection and response	Uptake of AI for cybersecurity, such as deployment of AI-based tools in Cross-border Cyber Hubs and CSIRTs for real-time cyber response capabilities
OPERATIONAL CYBERSECURITY	Development of frameworks for collaboration, for advanced operational cybersecurity, including CTI-based situational awareness, cyber/hybrid threat preparedness, expanded SOC/CSIRT capabilities, cyber crisis management and testing environments, including the digital twins of critical infrastructures and NIS2 essential and important entities.	Enhancement of threat detection and information sharing for national and cross-border Cyber Hubs to strengthen situational awareness and coordinated response capabilities at the EU-level
POST-QUANTUM CRYPTOGRAPHY (PQC)	Design and validation of quantum-resistant algorithms	Integration of PQC in European PQC testing infrastructure and Cyber Hubs to accelerate transition to quantum-safe systems

EU FUNDING IN PROMINENT STORIES

ESTABLISHING NATIONAL AND CROSS-BORDER CYBER HUBS	Cyber Hubs are designed to connect national capabilities, enabling real-time information sharing, joint situational awareness and coordinated incident response across MS. As these infrastructures mature, Cyber Hubs are expected to play a central role in implementing the Cyber Solidarity Act, supporting cross-border cooperation and enhanced situational awareness.
EUROPEAN PQC TESTING INFRASTRUCTURE	The planned deployment of a European testing infrastructure for post-quantum cryptography (PQC) will provide trusted, real-world testing environments accessible to industry, SMEs, public authorities and academia. This infrastructure is expected to accelerate market uptake of PQC technologies, support the implementation of the European PQC transition roadmap and strengthen EU's strategic autonomy in next-generation cryptographic solutions.
STRENGTHENING CYBERSECURITY IN EUROPEAN HEALTHCARE	Seven pilot projects are reinforcing the cybersecurity of hospitals and healthcare providers and are supporting the implementation of the action plan on cybersecurity in healthcare. These projects will deploy and validate tailored cybersecurity solutions, ranging from SOC services and threat intelligence to staff training, through real-world demonstrations in multiple MS.
REGIONAL CABLE HUBS FOR CRITICAL INFRASTRUCTURE PROTECTION	The establishment of Regional Cable Hubs strengthens the security and resilience of Europe's subsea cable infrastructure. By enabling near real-time threat detection, information sharing and coordinated response across MS, these hubs will enhance collective situational awareness and support the protection of critical connectivity assets.

3.5.3.2 National R&I ecosystems

Based on data from the EU-CSI, **the majority of Member States present an advanced posture in relation to the actions taken to identify, define, promote and support cybersecurity research and development priorities both at a national and international level.**



Cybersecurity in R&D priorities and initiatives

In all countries in the EU, national cybersecurity strategies cover R&I[157], although they are not always matched by an action plan, as reflected in the lack of a dedicated funding programme for cybersecurity in approximately one third of these countries (8). Still, since 2024, MS have improved the way in which such priorities are defined. Almost all MS have established a process to identify R&D priorities for cybersecurity (from 22 to 25 since 2024) and consider current and upcoming legislation (from 17 to 20), as well as EU strategic objectives (from 18 to 22).

This suggests an increasing coherence in the EU R&I landscape. In this context, the ECCC and the Network of National Coordination Centres (NCC) have a key role in aligning priorities, mobilising national ecosystems and strengthening the coherence of cybersecurity research, innovation and capability development across the EU. Grants from the NCC support the mobilisation of national cybersecurity ecosystems[158]. This mechanism significantly expands outreach and accelerates the uptake of cybersecurity solutions at national and regional level. It is interesting to note that there has also been a significant increase in the MS that have established start-up ecosystems at local and/or regional levels and other networking channels to foster innovation (from 18 to 23 since 2024).

157 ENISA, *NCSS Map*, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map (accessed 4 June April 2026).

158 Out of a total ECCC contribution of €87.86 million, €85.15 million was allocated to Financial Support to Third Parties (FSTP), enabling cascading funding for SMEs, start-ups and other stakeholders.

Policy Recommendations

Cybersecurity awareness and skills are a challenge for long-term resilience and require a balance of dedicated initiatives on awareness, education, talent hiring and retention, and continuous upskilling and reskilling, while considering the impact of AI.



Key recommendations:

- **[ENISA]** should monitor the impact of AI and emerging trends on cybersecurity skills. A contextualisation of ECSF-defined roles in the AI era could support the development of cybersecurity profiles with a stronger AI focus.
- **[The EC together with MS]** should strengthen public-private cooperation to reduce mismatches in cybersecurity skills and accelerate the integration of needed emerging skills through closer collaboration between education providers and industry.

Other recommendations:

- **[The EC together with MS]** should encourage organisations to embed cybersecurity in frameworks for corporate digital responsibility, with clearer accountability for cybersecurity practices, following approaches similar to ENISA's Awareness Raising-in-a-box[159].
- **[MS]** should support the integration of cybersecurity in primary and secondary education curricula through structured collaboration of national cybersecurity authorities and/or bodies with Ministries of Education, focusing on digital hygiene and online risks.
- **[The EC]** should include cybersecurity in the European Skills Intelligence Observatory[160] to ensure consistent and measurable data collection on gaps in cybersecurity skills and the factors influencing them over time.
- **[MS]** should encourage the attestation of cybersecurity skills to validate the proficiency of cybersecurity professional roles and help ensure that cybersecurity positions are filled by qualified personnel with an adequate skillset, while supporting the portability of skills across sectors.
- **[The EC and ECCC]** should strengthen the end-to-end innovation pipeline: Ensure continuity from research to deployment by better aligning Horizon Europe and Digital Europe actions, reducing the gap between low Technology Readiness Levels and operational uptake.

159 ENISA, *Cybersecurity Awareness Raising: The ENISA-Do-It-Yourself Toolbox*, available at https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box (accessed on 20/09/2026).

160 JRC, European Skills Intelligence Observatory (2026), available at https://publications.jrc.ec.europa.eu/repository/handle/JRC147054 (accessed on 20/09/2026).

IV.
Looking ahead

IV.
Looking Ahead

The overarching message of this Report is one of **cautious confidence**. The EU has demonstrated the political will and the capacity to cooperate to build a high common level of cybersecurity. Now it requires an acceleration of efforts. The challenge is to maintain the momentum with swiftness and flexibility to ensure the EU's readiness as the threat landscape and technology evolve.

Compared to the previous reporting period, the EU has experienced an overall improvement in terms of cybersecurity posture. The October 2024 transposition deadline of the NIS2 Directive played the role of a catalyst in national efforts devoted to structuring and operationalising the EU's cybersecurity governance. The priority for the period ahead lies in progressing the implementation of the legislative framework, including by addressing its more complex and demanding aspects.

The latter are especially important. Technological developments and shifts in global geopolitics are happening at an accelerated pace and with disruptive consequences: in 2026 alone the impact of frontier AI models on cybersecurity became increasingly apparent, while existing conflicts intensified and new ones took place. As uncertainty unfolds, cybersecurity remains a collective effort and the EU as a whole can provide a more solid front for what the future holds.

A Annex
Abbreviations

AI	Artificial intelligence
CABs	Conformity Assessment Bodies
CADA	Cloud and AI Development Act
CAN	CVE Numbering Authority
CER	Critical Entities Resilience
CERT-EU	Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies
CIRAS	Cybersecurity Incident Reporting and Analysis System
CPP	Cyber Partnership Programme
CRA	Cyber Resilience Act
CRA SRP	CRA Single Reporting Platform
CSA	Cybersecurity Act
CSA2	Cybersecurity Act Revision
CSIRT	Computer Security Incident Response Team
CSoA	Cyber Solidarity Act
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act
DSA	Digital Services Act
EC	European Commission
EC3	European Cybercrime Centre
ECCC	European Cybersecurity Competence Centre
ECSF	European Cybersecurity Skills Framework
EECC	European Electronic Communications Code
eIDAS	electronic IDentification, Authentication and trust Services
ENISA	European Union Agency for Cybersecurity
EPSS	Exploit Prediction Scoring System
ESAs	European Supervisory Authorities
ESMA	European Securities and Markets Authority
EU	European Union
EUCC	EU cybersecurity certification scheme on Common Criteria
EU-CSI	EU-Cybersecurity Index
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
EUDIW	EU Digital Identity Wallets
EUIBA	EU institutions, bodies, offices and agencies
EU-JCAR	EU Joint Cyber Assessment Reports
EUROPOL	European Union Agency for Law Enforcement Cooperation
EU-SCICF	EU Systemic Cyber Incident Coordination Framework
EUVD	European Vulnerability Database
FMIs	Financial Market Infrastructures
FSTP	Financial Support to Third Parties
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IICB	Interinstitutional Cybersecurity Board
ISACs	Information Sharing and Analysis Centres
ITSEFs	IT Security Evaluation Facilities

MICNET	Military Computer Emergency Response Team Operational Network
MS	Member States
MSSPs	Managed Security Service Providers
NATO	North Atlantic Treaty Organization
NCAF	National Capabilities Assessment Framework
NCCAs	National Cybersecurity Certification Authorities
NCCS	Network Code on Cybersecurity
NCCs	National Coordination Centres
NCSS	National Cyber Security Strategy
NIS CG	NIS Cooperation Group
NIS2	Network and Information Security Directive 2
OT	Operational Technology
PQC	Post-Quantum Cryptography
R&D	Research and Development
R&I	Research and Innovation
SIM	Security Incident Management
SOG-IS	Senior Officials Group – Information Systems Security
SPOC	Single Point of Contact
TI	Trusted Introducer
UCPM	Union Civil Protection Mechanism

B Annex

Deep-dive in sectorial maturity

Sectors of High Criticality and High Maturity

The **Telecoms**[161], **Electricity** and **Banking** subsectors remain the backbone of our economy and society. They feature high maturity and high criticality. Compared to the previous edition of the Report, three new sectors have joined this group, **Financial Market Infrastructures, Trust Services** and **Aviation**.

All the subsectors in this group have been regulated for many years, with strong oversight from authorities that have integrated cybersecurity into their supervisory activities and enhanced their expertise in this area. The sectors demonstrate advanced risk management, more consistent application of security measures and a higher level of operational preparedness compared to other sectors.

Sectors of High Criticality and Moderate Maturity above the Average

This category includes sub-sectors that are 'digital-by-default', namely providers of **Core Internet Services, Datacentre Services** and **Cloud Services**. Other sectors depend on these providers, making them crucial for the functioning of all other sectors. Their criticality is high, however their maturity is moderate despite already being above the overall average of sectors.

Like the first group of sectors, these sectors also demonstrate advanced risk management and strong management involvement, but apply security measures less consistently, and have a slightly lower level of operational preparedness. It is important to mention that the regulation of these sectors is complex, in particular when they are entwined with other sectors, as they may be subject to several sectoral legislations.

Sectors in the Risk Zone

The sectors and subsectors falling in the risk zone – namely **Health, Maritime, Railway, ICT Service Management,** Water (**Waste Water** and **Drinking Water**), **Public Administration**, and **Space** – are characterised by lower-than-average maturity, but with higher criticality relative to their maturity. In other words, these sectors are more critical to society and the economy than their preparedness to cope with cyber risks would suggest. Their maturity levels vary, because entities in these sectors differ in terms of their sizes and capabilities, while also being subjected to diverse legislations and varying exposure to cyber risks.

The **Health** sector is an attractive target due to its processing of sensitive data, as well as its increasing use of the Internet of Things and Internet of Medical Things systems, which increase the sector's exposure to threats. At the same time the entities under this sector struggle with foundational security measures, such as asset management, vulnerability management and data security. Most of these entities reported that current

161 Throughout this annex, the NIS2 Digital Infrastructure sector is represented by grouping its various entity types into subsectors, namely Core Internet Services, Telecoms, Cloud Services, Datacentre Services and Trust Services.

cybersecurity budgets are insufficient or only partially sufficient to meet their cybersecurity needs.

The **Maritime** and **Railway** subsectors operate in inherently complex environments comprising several stakeholders that typically interact closely with each other, e.g. infrastructure operators, transport service providers, technology providers etc. The reliance of these stakeholders on long-lived OT and IT systems as well as their dependence on supply chain and third-party providers contribute to their overall exposure to cyber threats. In addition, the sectors' increasing role in military logistics raises their strategic importance and potential attractiveness to intruders.

The maturity of the **ICT Service Management** sector remains at a moderate level, with modest and mostly ad-hoc progress over the past few years due to its inconsistent application of security measures and limited improvements in operational preparedness. For some entities, these challenges arise in foundational areas such as patch management, network segmentation or data security. For other entities, particularly those operating across borders, challenges are driven by complexities arising from coordinating response and recovery processes across different legal frameworks or jurisdictions. Such uneven implementation can be explained by the high diversity of the sector's entities, which vary in size, geographic scope and service models.

The **Public Administration** sector is still at an early stage of cybersecurity maturity, as it is a newly regulated sector. Its maturity is at the low-moderate level with reactive and uneven risk management and limited collaboration across the sector's entities. The sector is characterised by central, regional and local administrations and municipalities of varying sizes, which face different constraints on resources and expertise. This results in variations in the maturity levels of its various entities. The sector is also new to the supervisory authorities, which are only now becoming acquainted with its specificities and might be slow in providing sector-specific support.

The **Space** sector remains at the lower end of the moderate cybersecurity maturity level. This demonstrates large variability in terms of cybersecurity practices. This may in part be traced to the differing levels of obligations, oversight, guidance and prioritisation that it has experienced. Some entities fall within the scope of the NIS2 directive while others do not. Some entities have chosen to adopt applicable cybersecurity standards, while others have not. The implications of the sector's low to moderate cybersecurity maturity are significant, particularly given its growing role in supporting Europe's strategic autonomy[162], the increasing complexity of the space ecosystem and the ongoing transition to cloud infrastructures and software-defined nodes.

The Water sector (**Waste Water** and **Drinking Water** subsectors) is at low to moderate criticality and low to moderate maturity (depending on the subsector). The sector faces many challenges, including shortages of skilled personnel, insufficient budgets, risks from third-party suppliers, limited awareness and dependency on legacy systems. It is important to note that multiple entities in these sectors are small in size. These factors explain why entities in the sector struggle with implementing measures for the management of risk and have lower overall operational preparedness. Furthermore, engagement in initiatives for information sharing by entities in this sector appears to be lower in comparison to entities from other sectors.

Remaining sectors

The other sectors and subsectors are of moderate to low criticality and have moderate maturity. This group includes most subsectors of the Energy sector (**District Heating and Cooling**, **Oil**, **Gas** and **Hydrogen**) as well as the **Road** subsector. District Heating and Cooling, Oil, and Hydrogen remained stable in terms of cybersecurity maturity. But the gas sector strengthened its maturity and advanced within the moderate maturity band, meaning it has started moving out of the risk zone. Improved information sharing, stronger collaboration and better measures for the implementation of risk management drove this progress. The road subsector increased its maturity to a similar level as maritime, with progress largely driven by the automotive industry's strong practices in governance, risk management and comprehensive security assessments.

162 European Commission, *Autonomous Europe*, available at: https://defence-industry-space.ec.europa.eu/autonomous-europe_en (accessed 9 June 2026), Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023–2027 (IRIS²), Recital 55, available at: https://eur-lex.europa.eu/eli/reg/2023/588/oj/eng (accessed 9 June 2026).

C Annex

EU-Cybersecurity Index (EU-CSI) Indicators

In various sections of the report, data from EU-CSI indicators are presented to showcase the EU maturity level, the average EU score, as well as the number of MS on each maturity level as measured. This annex summarises the indicators that were included in the report, expanding on the description and meaning of each of those indicators.

SUPERVISION OF ESSENTIAL AND IMPORTANT ENTITIES

Indicator Description
This indicator measures the capability to identify, maintain a list of and collect required information on essential and important entities.

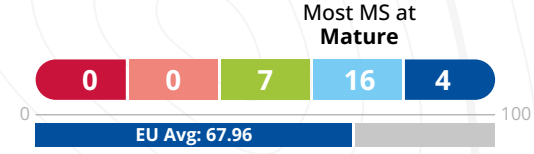
What 100 means?
A score of 100 means that, for all MS, almost all essential and important entities have been identified and supervisory measures are applied to them, including micro/small sized entities for whom specific processes have been established.



DEFINITION AND COMPLIANCE OF CYBERSECURITY RISK MANAGEMENT MEASURES FOR ESSENTIAL AND IMPORTANT ENTITIES

Indicator Description
This indicator measures the implementation of mandatory measures for the management of cybersecurity risk for essential and important entities, including related national legislation, data collection on compliance, definition of cybersecurity baseline(s), and mechanisms to check compliance.

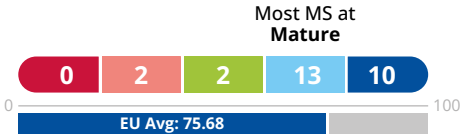
What 100 means?
A score of 100 means that for all essential and important entities, all measures for the management of cybersecurity risk are mandatory (across all MS legislation), compliance data is collected for the majority of the entities, cybersecurity baseline(s) are officially documented and periodically updated, and mechanisms to check compliance are in place.



COOPERATION AT NATIONAL LEVEL

Indicator Description
This indicator measures the definition and establishment of mechanisms for cooperation and information exchange between national competent authorities and/or bodies, for notifying cyber incidents and for identifying cyber threats.

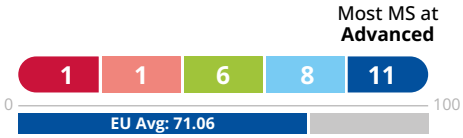
What 100 means?
A score of 100 means that all MS have established mechanisms for cooperation and information exchange of high maturity between their authorities, for notifying cyber incidents and identifying cyber threats.



INCIDENT REPORTING IMPLEMENTATION

Indicator Description
This indicator measures the definition and establishment of incident reporting procedure(s), including efforts in improving incident reporting, definition of incident classification taxonomies or thresholds for incident evaluation (at the national level).

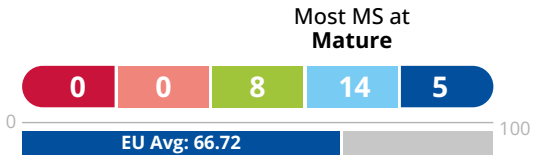
What 100 means?
A score of 100 means that secure reporting platforms, taxonomies and thresholds for cyber incidents have been defined, established, and regularly updated across all MS.



COVERAGE AND IMPLEMENTATION OF OBJECTIVES IN NATIONAL CYBERSECURITY STRATEGY

Indicator Description
This indicator measures the coverage and implementation of ENISA's 20 key national cybersecurity strategic objectives, including the presence of action plans and mechanisms for adaptive governance.

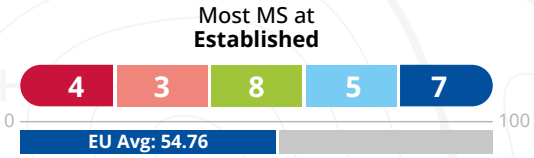
What 100 means?
A score of 100 means that all of ENISA's key national cybersecurity strategic objectives are fully covered by all MS, with fully implemented action plans and mechanisms for adapting them.



CSIRTS MATURITY

Indicator Description
This indicator measures the maturity level of CSIRTs participating in the CSIRT Network, focusing on their self-assessment based on ENISA's CSIRT Maturity Framework and peer-review processes.

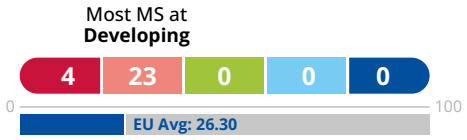
What 100 means?
A score of 100 means that all national CSIRTs that are part of the CSIRTs Network, have completed a self-assessment following ENISA's Maturity Framework achieving an "expert" maturity level also validated through a peer review.



PARTICIPATION BY ESSENTIAL/IMPORTANT ENTITIES IN INFORMATION SHARING ACTIVITIES

Indicator Description
This indicator measures the participation of essential and important entities in mutual and non-mandatory cybersecurity-related information-sharing activities.

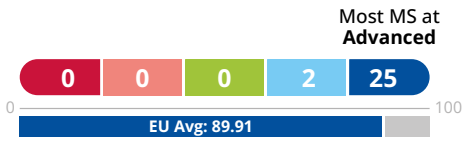
What 100 means?
A score of 100 means that, across all MS, all surveyed entities participate in information sharing as part of a National ISAC, an EU-ISAC, and/or an industry association.



SUPPLY CHAIN MANAGEMENT PRACTICES BY ESSENTIAL/IMPORTANT ENTITIES

Indicator Description
This indicator measures the adoption of supply chain management practices by essential and important entities.

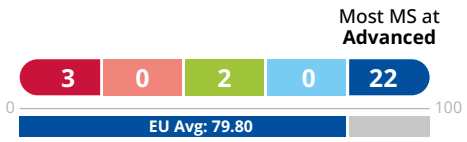
What 100 means?
A score of 100 means that, across all MS, all surveyed entities have specific practices for supply chain management in place.



COVERAGE OF VULNERABILITY DISCLOSURE POLICIES

Indicator Description
This indicator measures the implementation of policies for the coordinated disclosure of vulnerabilities as well as their coverage of critical sectors.

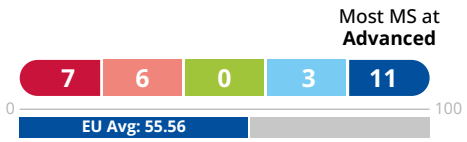
What 100 means?
A score of 100 means that policies for the coordinated disclosure of vulnerabilities have been implemented and cover all critical sectors in NIS2 across all MS.



NATIONAL CERTIFICATION CAPABILITIES

Indicator Description
This indicator measures the capabilities in cybersecurity certification for both national and European schemes.

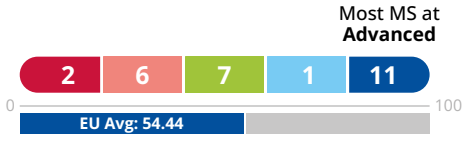
What 100 means?
A score of 100 means that all MS have at least one national cybersecurity certification scheme while also have accredited or are in the process of accrediting an EUCC certification body and an EUCC evaluation facility.



CYBERSECURITY IN NATIONAL EDUCATION CURRICULA

Indicator Description
This indicator measures the actions taken to integrate and enhance cybersecurity curricula in primary and secondary education.

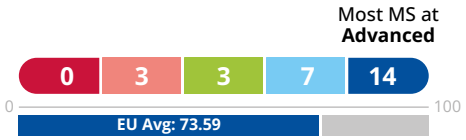
What 100 means?
A score of 100 means that all MS have integrated cyber-security curricula into primary and secondary education and update them regularly.



CYBERSECURITY IN HIGHER EDUCATION

Indicator Description
This indicator measures the actions taken to include, promote and enhance cybersecurity in higher levels of education.

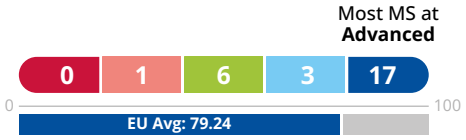
What 100 means?
A score of 100 means that all MS have implemented all relevant measures to promote, include and enhance cybersecurity in higher levels of education.



CYBERSECURITY IN R&D PRIORITIES AND INITIATIVES

Indicator Description
This indicator measures the actions taken in relation to identifying, defining, promoting and supporting cybersecurity research and development priorities both at a national and international level.

What 100 means?
A score of 100 means that for all MS cybersecurity priorities are identified and defined, multiple support mechanisms have been established, and all MS engage in international R&D activities.



TP-01-26-024-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ISBN 978-92-9204-816-7

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union