POLICY BRIEF

ENISA: Fit for Purpose?

Reviewing the EU Cybersecurity Agency's Role in an Evolving Policy Ecosystem

Christina Rupp

March 20, 2025

Tech analysis and policy ideas for Europe

interface

Table of Contents

Executive Summary

Since its inception 20 years ago, the European Union Agency for Cybersecurity (ENISA) has evolved and gained prominence as a cybersecurity entity at EU level. ENISA is entrusted with a central role in implementing EU cybersecurity policies, fostering cooperation among Member States, and strengthening resilience against cyber threats. In recent years, its mandate has expanded and the agency has taken on an increasingly multifaceted role as the EU pursues an ambitious political and regulatory cybersecurity agenda. With legislation such as the NIS2 Directive, the Cyber Resilience Act, and the Cyber Solidarity Act, ENISA's workload has grown substantially, placing additional demands on the agency. This raises questions about whether the agency is sufficiently equipped to manage an expanding portfolio of tasks amidst a growing threat landscape – in short, **is ENISA fit for purpose?**

The paper identifies six challenges facing ENISA in the fulfillment of its purpose:

1. ENISA operates within a complex and heterogeneous environment, where its role and influence are contested by the emergence of new cybersecurity entities at the EU level. At the same time, the agency must demonstrate added value in a landscape marked by varying levels of maturity and differing approaches to implementing EU cybersecurity policies across Member States.
2. ENISA's expansion of tasks results in mounting expectations from a steadily increasing number of actors, as the agency must cater to a complex actor network while facing rising demands from various stakeholder groups, such as EU Institutions, Bodies, and Agencies; Member State entities, and private sector actors.
3. ENISA's activities extend beyond purely internal market-driven objectives as the agency's operational footprint continues to grow. As cybersecurity is an area where national and EU-level security concerns increasingly intersect, ENISA's involvement in incident management, situational awareness, and operational coordination-related activities has also grown. These activities contribute to, but also go beyond, the agency's primary objective of supporting the EU's internal market, which forms its legal basis.
4. ENISA's purview is progressively shaped by political dynamics, as reflected by the increasing relevance of cybersecurity to EU policy-making, the agency's growing role in policy development, ENISA's expanded participation in the Council of the EU's Horizontal Working Party on Cyber Issues, and the political controversies that have arisen surrounding cybersecurity certification schemes developed by ENISA.
5. ENISA is taking on a more prominent role at the international level, inter alia, by establishing working arrangements with cybersecurity entities of international partners, participating in EU cyber dialogues with foreign counterparts, and managing a growing number of collaboration requests emanating from outside the EU.
6. ENISA's workforce needs exceed its allocated budget, as the agency's resource requests go unmet amid expanding responsibilities from new legislation, rising stakeholder expectations, and a deteriorating cybersecurity threat landscape.

These challenges underscore the increasing complexity and scope of ENISA's tasks, as the agency must, inter alia, address diverse priorities while ensuring

interoperability across Member States, reconcile EU-level coordination with national sovereignty, and balance its technical mandate with political realities. All of these tasks ultimately constrain the agency's ability to contribute to implementing the EU cybersecurity policy framework and support policy coherence.

To address these challenges, the paper puts forward three recommendations:

- **Clarifying ENISA's role**: To optimize its impact, particularly given its limited resources, policy- and decision-makers should clarify the agency's role and specify where ENISA adds the most value in enhancing the Union's cybersecurity.
- **Refining prioritization of ENISA activities:** Improved prioritization would enable ENISA to sustainably build specialized expertise in key areas while fostering trusted relationships with priority recipients of its actions.
- **Managing expectations of ENISA's target audiences:** To ensure transparency and clarity, it is crucial that stakeholders understand how ENISA prioritizes its activities and engagement as this will mitigate potential misunderstandings and manage expectations based on a realistic understanding of the agency's capabilities.

With ENISA's role under review as part of the European Commission's ongoing evaluation mandated by the Cybersecurity Act, 2025 marks a pivotal moment for reassessing the agency's capacity and clarifying its strategic direction. For policymakers in Member States and EU institutions, two basic conceptual options emerge to make ENISA truly fit for purpose: **equipping ENISA with additional financial resources and personnel to fully meet its mission and responsibilities** or **redefining ENISA's mandate to align with existing resources**, which would entail significantly narrowing the agency's tasks and scope of activities. Taking the necessary steps to act on one of the proposed options, rather than maintaining the below-par status quo, is essential if the EU is to effectively manage and implement its ever-expanding cybersecurity policy framework.

Disclaimer: The paper's recommendations were developed prior to the publication of ENISA's 2025-2027 Single Programming Document in February 2025. This document may signal a shift in the agency's approach, with a focus on de-prioritization and a reorganization of ENISA's internal structure. It remains to be seen whether these changes, which support some of the paper's recommendations, will yield the desired outcomes by alleviating the agency's long-standing challenges.

Introduction

In 2004, the European Union (EU) established the European Network and Information Security Agency (ENISA), now headquartered in Athens, Greece.[1] Since then, the agency's name has been changed to the European Union

Agency for Cybersecurity, while its abbreviation remains intact. EU Member States, the Commission, and the European Parliament have also gradually expanded ENISA's mandate and tasks in both quantitative and qualitative terms, reflecting the rising prominence of cybersecurity on the EU's agenda in recent years.[2]

In the first ten years of the agency's existence, the EU's regulatory entrepreneurship[3] efforts – proactive initiatives to shape and expand the cybersecurity policy ecosystem through regulation and policy – in the area of cyber and IT security were still very limited. Over the past decade, however, the EU has developed likely the world's most comprehensive regulatory framework on cybersecurity through the adoption of numerous cybersecurity-specific horizontal and sectoral directives and regulations as well as policies spanning numerous policy areas.[4]

In particular, the last few years have witnessed an unprecedented dynamic in regulatory activity, with more than 300 legal acts mentioning cybersecurity adopted between 2019 and 2024.[5] This evolution has had implications for ENISA: the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive),[6] the Cyber Resilience Act (CRA),[7] and Cyber Solidarity Act (CSOA)[8] are just three examples of recent legislative EU endeavors that have conferred additional tasks on the agency.[9]

Among some of ENISA's recently added tasks feature

- the development and maintenance of a "European vulnerability database"[10] (Art. 12(2) NIS 2 Directive),
- the drafting of a biennial "report on the state of cybersecurity in the Union" (Art. 18 NIS 2 Directive, the first of which was published in December 2024[11]),
- the "[e]stablishment of a single reporting platform" (Art. 16(1) CRA)[12], inter alia, for

1 ENISA (2024): New chapter begins as ENISA celebrates 20 years of strengthening cybersecurity.

2 For example, in 2022, the European Commission stated that "cybersecurity has become a top political and operational priority of the European Commission," European Commission (2022): Replies of the European Commission to the European Court of Auditors' Special Report 'Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats'.

3 The term *normative entrepreneurship* was coined by Finnemore and Sikkink in Martha Finnemore and Kathryn Sikkink (1998): International Norm Dynamics and Political Change, International Organization 52(4).

4 Christina Rupp (2024): Navigating the EU Cybersecurity Policy Ecosystem, interface.

5 The number is based on the results for a keyword search in EUR-Lex for "cyber security" or "cybersecurity" excluding corrigenda and filtering by legal acts. In total, there are 313 results for the timeframe 2019–2024 (2019: 31; 2020: 34; 2021: 54; 2022: 56; 2023: 68; 2024: 70).

6 Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), 2022/2555.

7 Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), 2024/2847.

8 Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act), 2025/38.

9 Other recent legislation also mentioning and conferring tasks to ENISA includes the Commission Delegated Regulation establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, 2024/1366 and Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, 2023/2841.

10 In this context, see also Alexander Martin (2024): EU cyber agency will not create active vulnerability database, says chief cybersecurity officer, The Record.

11 ENISA (2024): 2024 Report on the State of the Cybersecurity in the Union.

12 See also Tenders Electronic Daily (2025): Implementation of the Single Reporting Platform, ENISA/2025/OP/0001.

the notification of "actively exploited vulnerabilit[ies] contained in the product with digital elements" (Art. 14(1) CRA) and "severe incident[s] having an impact on the security of the product with digital elements" (Art. 14(3) CRA) by manufacturers pursuant to the CRA,

- the "operation and administration of the EU Cybersecurity Reserve, in full or in part" (Art. 14(5) CSOA) through the CSOA, as well as
- upon request by either the European Commission or the European cyber crisis liaison organisation network (EU-CyCLONe), the "review and assess[ment of] cyber threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant cybersecurity incident or large-scale cybersecurity incident" (Art. 21 CSOA) in the framework of the EU's European Cybersecurity Incident Review Mechanism established via the CSOA.

Even if more and more voices in the policy world are calling for the existing initiatives to be properly implemented first,[13] cybersecurity will likely continue to be high on the political agenda during the term of this European Commission. Looking at Ursula von der Leyen's candidate speech for a second mandate as European Commission President,[14] the political guidelines for the von der Leyen Commission II,[15] and the mission letter to the new Executive Vice-President for Tech Sovereignty, Security and Democracy Henna Virkkunen also overseeing the 'cyber portfolio,'[16] all indicate that cybersecurity will most likely keep its place at the higher end of the EU's political agenda.[17] Most recently, for example, the European Commission's action plan on the cybersecurity of hospitals and healthcare providers followed through on this indication by proposing to task ENISA with "establish[ing], within its organisation, a dedicated European Cybersecurity Support Centre for hospitals and healthcare providers as part of its mandate to safeguard and support the EU's critical infrastructure."[18] Expectations facing ENISA are thus likely to continue rising, from the European Commission, Member States, as well as other stakeholders, raising questions about whether the agency is sufficiently equipped to manage an expanding portfolio of tasks amidst a growing threat landscape – in short, whether the agency is fit for purpose.

ENISA's ability to fully deliver on its mandate is not an end in itself. Instead, an ENISA that is fit for purpose is imperative to the EU's strategic ambition to enhance

13 See, for example, Netherlands (2024): Effective EU cybersecurity legislation and decisive diplomacy in the cyberdomain.

14 European Commission (2024): Statement at the European Parliament Plenary by President Ursula von der Leyen, candidate for a second mandate 2024-2029.

15 European Commission (2024): Political Guidelines 2024-2029.

16 European Commission (2024): Mission Letter to Henna Virkkunen.

17 Specifically, von der Leyen aims to enhance the EU's cybersecurity-related work in the context of defense and the health sector. In her political guidelines, she also notes exploration of the EU's sanctions framework, and in a letter to now Commissioner Virkkunen, the need both to "improv[e] the adoption process of European cybersecurity certification schemes" and for more inward-looking tasks to "ensure that the Commission becomes more resilient to cybersecurity threats."

18 European Commission (2025): European action plan on the cybersecurity of hospitals and healthcare providers and ENISA (2025): Proposed ENISA role to safeguard cybersecurity of health sector. For an overview of tasks for ENISA, see especially p. 7 of the action plan, which includes the development of procurement guidelines, the creation of an ENISA-sponsored European Known Exploited Vulnerabilities catalogue for medical devices, electronic health record systems, and providers of ICT equipment and software in health, as well as the facilitation of a wide roll-out of national cybersecurity exercises.

cybersecurity across the Union as well as its regulatory and policy innovation on cybersecurity. Internally, an ENISA unfit for purpose could impair EU-level efforts to create a cohesive and effective cybersecurity framework, as the success of Union-wide cybersecurity policies also relies on coordination across Member States, with ENISA entrusted with an essential role in supporting this effort. Externally, if ENISA struggles to deliver on its mandate, including by supporting improved coordination and consistent implementation, this may have broader implications for the EU's standing as a regulatory entrepreneur and for its often invoked *Brussels Effect*, a term coined to refer to the "EU's unilateral ability to regulate global markets by setting the standards" in various policy fields.[19]

This makes 2025 a pivotal moment to assess the agency's role and capacity within the EU cyber ecosystem – also as it coincides with the European Commission's ongoing evaluation of the agency, mandated by Article 67 of the Cybersecurity Act (CSA),[20] which could prompt the European Commission to propose a revision of ENISA's mandate. Testaments to the need to evaluate ENISA include the recently adopted Council conclusions on ENISA[21] from December 2024 as well as the earlier June 2024 Council conclusions on the future of cybersecurity, which, inter alia, called upon the European Commission "to take duly into account the development of ENISA's role reviewing the Cybersecurity Act" and ENISA "to establish clear priorities, including focusing on supporting the Member States through existing structures."[22] Most recently, in March 2025, the EU ministers responsible for cybersecurity emphasized the "need for a strengthened, clearly defined, and focused ENISA [...] mandate" as a component of their 'Warsaw Call' declaration.[23]

This policy paper aims to contribute to evaluative efforts at the policy level by reviewing ENISA's capability to fulfill its mandate in an increasingly complex cybersecurity landscape. The analysis approaches the question of ENISA's 'fitness' by examining key factors and capabilities necessary to achieve the agency's purpose, including the scope of tasks assigned to ENISA, staffing, budget, and governance structures (Chapter 3). The paper also explores the agency's role within the broader EU cybersecurity policy framework, ENISA's actor network and target audiences, its position in political processes, as well as its international engagement. By considering the implications of these considerations, the paper identifies challenges to the agency's ability to fulfill its purpose and meet the expectations placed upon it (Chapter 4), underscoring the importance of clearly defining the agency's role, more

19 Anu Bradford (2021): The European Union in a globalised world: the "Brussels effect," Revue Européenne du Droit 2.
20 The results of the evaluation were originally due by June 2024 (Art. 67(1) CSA).
21 Council of the EU (2024): Council conclusions on ENISA, 16527/24.
22 Council of the EU (2024): Council Conclusions on the Future of Cybersecurity: implement and protect together, 10133/24.
23 Polish Presidency of the Council of the European Union (2025): Warsaw Call Declaration adopted at the informal TTE Telecom Council on cybersecurity.

effectively articulating its priorities, and enhancing the management of stakeholder expectations when looking ahead (Chapter 5).

ENISA 101: Answers to Frequently Asked Questions

What are the main characteristics of decentralized EU agencies like ENISA?

ENISA was established as a decentralized EU agency. The CSA draws on Article 114 of the Treaty on the Functioning of the European Union (TFEU),[24] providing the opportunity for the European Parliament and the Council of the European Union to adopt measures deemed necessary "for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the **establishment and functioning of the internal market**" (Art. 114(1) TFEU).[25]

Being a decentralized agency – as opposed to an EU executive, Common Foreign and Security Policy (CFSP) or European Atomic Energy Community agency[26] – comes with specific characteristics:

- **Establishment:** Decentralized EU agencies are established "by secondary law to manage specific technical, scientific or managerial tasks," have their own legal personality, are set up indefinitely timewise, and are located in Member States throughout the Union.[27]
- **Function:** In general terms, decentralized agencies are tasked to "contribute to the implementation of EU policies and support cooperation between the EU and national governments by pooling technical and specialist expertise and knowledge from both the EU institutions and national authorities."[28]
- **Oversight:** Decentralized EU agencies are "subject to the external control of the Court of Auditors and to the annual discharge from the European Parliament."[29]
- **External engagement:**[30] The external relations of decentralized EU agencies have been

24 The previous regulations specifying ENISA's mandate also drew on this legal basis.

25 The TFEU defines the internal market as "an area without internal frontiers [… permitting] the free movement of goods, persons, services and capital" (Art. 26(2) TFEU).

26 See European Union (n.d.): Types of institutions and bodies for further information on their characteristics.

27 EUR-Lex (n.d.): European Union agencies. See also European Parliament, Council of the EU, and European Commission (2012): Joint Statement on decentralised agencies.

28 EUR-Lex (n.d.): European Union agencies.

29 European Commission (2019: EU Budget Glossary.

30 In 2012, the European Parliament, the Council of the EU, and the European Commission agreed on a 'common approach' on decentralized agencies. With respect to the international dimension of an EU agency's activities, the common approach notes that "an early exchange of information should take place on respective international activities between agencies, the Commission and the relevant EU Delegations, to ensure the consistency of EU policy," European Parliament, Council of the EU, and European

described as a "constitutional twilight zone," given the fact that they bring "together two constitutionally problematic issues: the EU's external action and the limits to the empowerment of EU agencies."[31] This results in a circumscribed, narrow scope for external action. For example, decentralized agencies must respect and maintain the EU's "institutional balance,"[32] and any agency's external engagement should be essential to fulfilling its core responsibilities. The procedures for the external activities of specific EU agencies are outlined in agreements between the relevant Commission Directorate-Generals (DGs) and the agencies.[33]

What is ENISA's purpose?

ENISA's purpose is threefold (emphasis by the author):

1. "achieving a **high common level of cybersecurity** across the Union,"
2. "**reducing the fragmentation of the internal market**," and
3. "**approximating Member State laws**, regulations and administrative provisions" (Art. 3)

as outlined at the beginning of the CSA.

As also contained in the CSA, EU co-legislators envision the agency to be "a **centre of expertise on cybersecurity** by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks" (Art. 4(1)). In July 2020, ENISA published its strategy for "A Trusted and Cyber Secure Europe" outlining seven strategic objectives that are linked to specific CSA articles and activities.[34] In February 2025, the agency published an updated version of its strategy, as revised by its Management Board in October 2024.[35] With some minor adjustments in wording, the seven strategic objectives remained primarily the same. The major change rests in clustering them in horizontal and vertical objectives as well as an increased

Commission (2012): Joint Statement on decentralised agencies. The implementation report on the implementation of the Joint Statement and Common Approach on the location of the seats of decentralized agencies can be found here: European Commission (2019): Report on the implementation of the Joint Statement and Common Approach on the location of the seats of decentralised agencies, COM(2019) 187 final.

31 Merijn Chamon (2019): A constitutional twilight zone: EU decentralized agencies' external relations, Common Market Law Review 56(6).

32 For instance, this institutional balance includes that "EU agencies may not affect the prerogative of the Council to determine the (external) policy of the Union" and EU agencies act based on the recognition that the "Commission has a prerogative and duty to represent the EU to the outside world," while at the same time acknowledging "the Parliament's prerogatives when engaging in external relations," Merijn Chamon (2019): A constitutional twilight zone: EU decentralized agencies' external relations, Common Market Law Review 56(6).

33 Merijn Chamon (2019): A constitutional twilight zone: EU decentralized agencies' external relations, Common Market Law Review 56(6). For example, such a working arrangement may include provisions specifying "a requirement to copy the partner DG in all formal correspondence with third countries' authorities". Chamon also noted that ENISA is among the EU agencies not permitted to directly communicate with the EEAS, since "all communication with the EEAS must go through the partner DG" – it is unclear to the author if this arrangement still holds today.

34 ENISA (2020): ENISA Strategy - A Trusted and Cyber Secure Europe and ENISA (2020): ENISA unveils its New Strategy towards a Trusted and Cyber Secure Europe.

35 ENISA (2025): ENISA Strategy - A Trusted and Cyber Secure Europe.

emphasis on implementation in the second as well as preparedness and response in the third objective (see below).[36] According to the strategy, ENISA seeks to achieve and contribute to the following objectives through its activities:

→ **Horizontal objectives**:

- Empowered communities in an involved and engaged cyber ecosystem
- Foresight on emerging and future cybersecurity opportunities and challenges
- Consolidated and shared cybersecurity information and knowledge support for Europe

↓ **Vertical objectives:**

- Support for effective and consistent **implementation** of EU cybersecurity policies
- Effective Union **preparedness and response** to cyber incidents, threats, and cyber crises
- Strong cybersecurity capacity within the EU
- Building trust in secure digital solutions

What is ENISA tasked with?

The CSA assigns ENISA eight activity areas:

(1) Development and implementation of Union policy and law (Article 5)

- Provision of "independent opinion and analysis as well as carrying out preparatory work" to "assist[…] and advis[e] on the development and review of Union policy and law in the field of cybersecurity and on sector-specific policy and law initiatives,"
- Issuance of "opinions, guidelines, provi[sion of] advice and best practices" in an assistance effort towards Member States to "implement the Union policy and law regarding cybersecurity consistently,"
- Support to NIS Cooperation Group activities,
- Support to Member States "in the implementation of specific cybersecurity aspects of Union policy"

(2) Capacity-building (Article 6)

- Assistance to Member States with regard to
  - "efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents [through] knowledge and expertise,"
  - "developing national CSIRTs [Computer Security Incident Response Teams]," and
  - "regularly organising the cybersecurity exercises at Union level"
- Assistance to Member States and EU Institutions, Bodies and Agencies (EUIBAs) with

36 Aside from visually representing these objectives as horizontal or vertical, ENISA does not provide a definition for both qualifiers.

regard to "establishing and implementing vulnerability disclosure policies on a voluntary basis"

- Assistance to EUIBAs with regard to
  - "improv[ing] the prevention, detection and analysis of cyber threats and incidents and to improve their capabilities to respond to such cyber threats and incidents, in particular through appropriate support for the CERT-EU [Cybersecurity Service for the Union institutions, bodies, offices and agencies]," and
  - "developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking the progress in their implementation"

(3) Operational cooperation at the Union level (Article 7)

- Vis-à-vis Member States through the CSIRTs Network:
  - "advising on how to improve their capabilities to prevent, detect and respond to incidents and, at the request of one or more Member States, providing advice in relation to a specific cyber threat" and
  - "analysing vulnerabilities and incidents on the basis of publicly available information or information provided voluntarily by Member States for that purpose"
- Vis-à-vis Union and Member States: "contribut[ing] to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity," for example, by "ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs network and the technical and political decision-makers at Union level"
- Vis-à-vis EUIBAs:
  - "exchang[ing] know-how and best practices"
  - providing "advice and issuing of guidelines on relevant matters related to cybersecurity"

(4) Market, cybersecurity certification, and standardization (Article 8)

- Preparation of "candidate European cybersecurity certification schemes"
- Development and publication of "guidelines and develop good practices, concerning the cybersecurity requirements for ICT [information and communications technology] products, ICT services and ICT processes"

(5) Knowledge and information (Article 9)

- Provision of "topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity"
- Performance of "long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents"

(6) Awareness-raising and education (Article 10)

Implementation of "regular outreach campaigns to increase cybersecurity and its visibility in the Union and encourage a broad public debate" together with Member

States and EUIBAs

(7) Research and innovation (Article 11)

- Provision of advice to EUIBAs and Member States on "research needs and priorities in the field of cybersecurity"
- "Contribut[ion] to the strategic research and innovation agenda at Union level in the field of cybersecurity"

(8) International cooperation (Article 12)

- Supporting "the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation"

These activity areas translate to various operational activity areas outlined in ENISA's annual work programs.[37]

How is the European Commission involved in ENISA's governance structures and day-to-day operations?

In contrast to EU executive agencies placed directly under the European Commission's control and oversight,[38] the relationship of decentralized EU agencies with the European Commission is one of "partial autonomy," manifested, for example, in the European Commission's involvement in the drafting of the agency's work program or the representation in statutory bodies of the respective agencies.[39] The Directorate-General for Communications Networks, Content and Technology (DG CONNECT) is the DG responsible (partner DG) for ENISA. The European Commission is involved in ENISA's governance structures at multiple levels: It participates in ENISA's **Management and Executive Boards** (through representatives from DG CONNECT and Directorate-General for Digital Services (DG DIGIT[40])), with voting rights and the authority to request extraordinary meetings, proposes **Executive Director** candidates, and evaluates their performance. It also oversees ENISA's strategic direction through mandatory consultations on financial rules, **annual work programs**, and the **single programming document**, where the European Commission's opinion must be considered before adoption. Furthermore, ENISA is

37 ENISA's most recent 2025 work program can be found here.
38 European Commission (2019): EU Budget Glossary.
39 Edoardo Chiti (2018): Decentralized Implementation: European Agencies, in: Oxford Principles of European Union Law: The European Union Legal Order: Volume I.
40 ENISA (2025): List of ENISA Management Board Representatives and Alternates and ENISA (2025): Executive Board Representatives and Alternates.

required to submit various reports to the European Commission, including biennial progress updates, annual budgetary reports, and responses to audit observations. Additionally, the European Commission evaluates ENISA's impact, mandate, and future tasks every five years and retains the authority to propose amendments to the regulatory framework stipulating its mandate. Vice versa, the European Commission relies on ENISA for technical advice and analyses to support cybersecurity policy development and implementation and may request ENISA to create or review European cybersecurity certification schemes under the Union's rolling work program. For more details and references to the relevant provisions of the CSA, see Annex I (Section 6.1).

How are EU Member States involved in ENISA's governance structures and day-to-day operations?

The relationship between ENISA and EU Member States is structured to ensure Member States are involved in the agency's governance and advisory processes. Each Member State is represented in ENISA's **Management Board**, with one appointed member per state, all possessing voting rights. This arrangement ensures that Member States collectively hold influence on ENISA's strategic decisions, such as the adoption of its **single programming document** and **budget**. Some Member States are also represented in ENISA's **Executive Board**, which handles preparatory and administrative tasks to facilitate Management Board decision-making. Additionally, representatives of each Member State are involved in ENISA's **National Liaison Officers Network** (NLO), which supports the exchange of information between ENISA and Member States. Finally, Member States have the right to attend and participate in meetings of ENISA's **Advisory Group**, which provides expert guidance on ENISA's work. For more details and references to the relevant provisions of the CSA, see Annex I (Section 6.1).

Who decides on ENISA's resource allocation?

Article 314 TFEU outlines the EU's budgetary procedure, which is decided annually by the European Parliament and the Council of the EU through a special legislative procedure.[41] The annual budget must follow the EU's Multiannual Financial Framework (MFF), which sets spending limits by category and is approved by the

41 For an explanation of the EU special legislative procedure and its distinction from the ordinary legislative procedure, see EU Legislation and Policies: A Basic Explainer, in: Christina Rupp (2024): Navigating the EU Cybersecurity Policy Ecosystem, interface.

Council of the EU with involvement from the **European Parliament** (Art. 312 TFEU). The current MFF covers the years 2021-2027. The **European Commission** prepares both the MFF proposal and draft annual budgets, based on estimates received from EU institutions and bodies (see Art. 29 CSA for ENISA's procedure). If the European Parliament and the Council of the EU disagree on the budget, Article 314(5)–(8) TFEU describe resolution steps, including forming a conciliation committee. **ENISA's Executive Director** is responsible for managing the agency's budget (Art. 31(1) CSA).

How have ENISA's budgetary and human resources evolved over time?

In 2023, ENISA oversaw a budget of 44 million euros (including 15 million euros for implementation of the Cybersecurity Support Action through a separate contribution agreement[42]) and employed 113 people.[43] In addition to its regular budgetary allocation and additional funding for the implementation of the Cybersecurity Support Action until 2026, ENISA receives supplementary financial means for carrying out specific tasks: 12 million euros for establishing, managing, and maintaining the single reporting platform foreseen in the CRA as well as 2.55 million euros in order to continue the Cybersecurity Support Action until December

42 In May 2022, EU Member States agreed on the establishment of an "Emergency Response Fund for Cybersecurity" as a reaction to Russia's war against Ukraine (Council of the EU (2022): Nevers Call to Reinforce the EU's Cybersecurity Capabilities). Subsequently, ENISA was tasked with implementing the so-called Cybersecurity Support Action as a pilot project "to help further mitigate the risks of large-scale cybersecurity incidents in the short term, both by preventive [ex-post] and reactive [ex-ante] services, which are offered free of charge" (Centre for Cybersecurity Belgium (2022): ENISA launches Pilot Project for Emergency Measures). Addressees of these services are the "Member States' NIS2 Directive entities," which include, for example, support in the area of incident coordination, cybersecurity exercises, or crisis communication (ENISA (2023): Cybersecurity Support Action). To implement the pilot Cybersecurity Support Action, ENISA has received an additional contribution totaling 15 million euros. Upon conclusion of the pilot, funding granted from the Digital Europe Programme permits ENISA to continue the action until 2026. To this end, ENISA opened a public tender amounting to roughly 28 million euros with the intention of concluding "framework service contracts under 28 Lots with economic operators capable to support ENISA in the delivery of cybersecurity services in every EU Member State as well as across EU" (900,000 euros per Member State (lots 1–27) and 4 million euros for EU-wide services (lot 28) (Tenders Electronic Daily (2024): Supporting ENISA for the provision of cybersecurity services to European Union Member States, ENISA/2024/OP/0005). Therefore, it should be emphasized that ENISA assumes a coordinating function, but is not implementing these services itself. ENISA's 2023 Coordinated Activity Report enumerates that the 2023 implementation of the Cybersecurity Support Action resulted in "185 pen tests, 54 exercises, 25 threat landscape reports, incident response support in 16 MSs, risk monitoring for 19 MSs, [and] training for 25 MSs" (ENISA (2024): ENISA Consolidated Annual Activity Report 2023).

43 While noting that the numbers cannot be directly compared, as entities undertake different tasks, for contextualization, CERT-EU, in contrast, has a budget of about 9 million euros in 2025 (Maximilian Henning (2024): Weniger Geld für Forschung, mehr für Sicherheit, Tagesspiegel and European Commission (2024): Statement of estimates 2025) and employs 45 staff (Paul Dalg (2024): EU-Budget: Institutionen bereiten Cyber-Compliance vor, Tagesspiegel). In recent years, CERT-EU's budget increased from 2 million euros in 2022 (European Commission (2021): Statement of estimates 2022) and 5.3 million euros in 2023 to 7.8 million euros in 2024 (European Commission (2023): Statement of estimates 2024). The ECCC intends to have 38 posts filled in the next year and disposes of a total budget of roughly 195 million euros (including the money allocated to it via Digital Europe and Horizon Europe, European Commission (2024): Draft General Budget - Working Document III). Compared to other cybersecurity agencies or entities at the national level worldwide where information is publicly available, ENISA's budgetary resources are rather slim; see, for example, Adam Janofsky (2021): Countries are increasing their cyber response budgets — but spending still varies widely, The Record and U.S. Department of Homeland Security (2024): Testimony of Jen Easterly on Fiscal Year 2025 Budget for the Cybersecurity and Infrastructure Security Agency. Of all the EU's decentralized agencies (33 in total), in 2023, ENISA ranks 23rd in terms of the number of staff and 25th regarding the budgetary amount at its disposal (European Court of Auditors (2024): Annual report on EU agencies for the financial year 2023). In the same year, of the 11 decentralized agencies financed under the EU's Multiannual Financial Framework heading 1 ("Single market, innovation and digital"), ENISA ranks 10th in terms of both the number of staff and budgetary expenditure.

2027.[44] According to the agency's latest single programming document, other contribution agreements are on the table regarding the agency's tasks in the context of the Cyber Situation and Analysis Centre[45] and the Cyber Reserve as stipulated in the CSOA.[46]

The following two figures provide an overview of developments in 2005–2023 based on data from the European Court of Auditors (ECA)[47]:

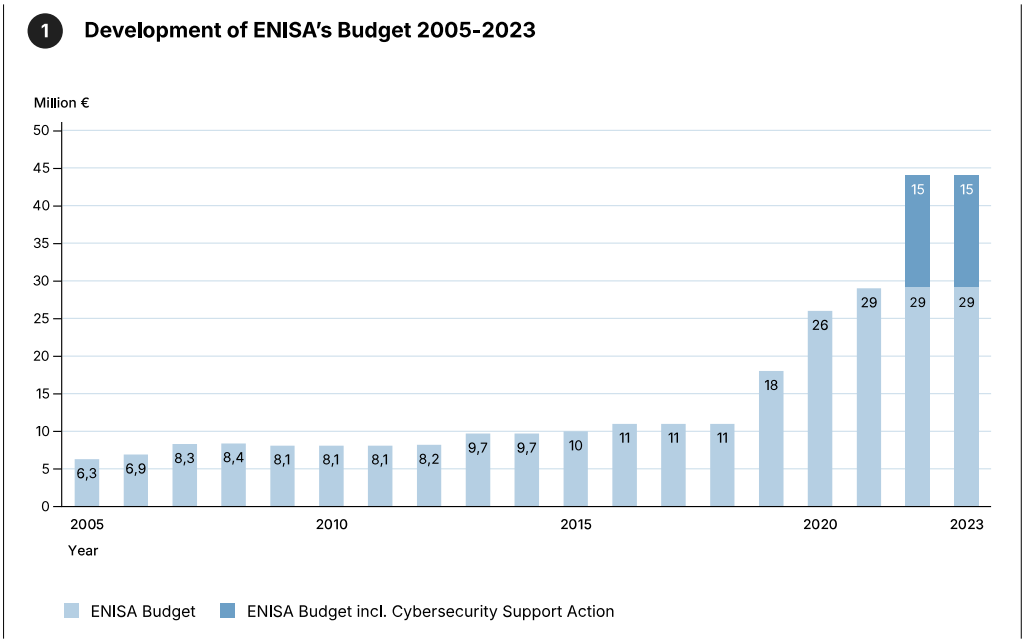

Figure 1: Development of ENISA's budget 2005–2023

44 ENISA (2025): ENISA Single Programming Document 2025-2027.

45 For more details on the Cyber Situation and Analysis Centre, see Section 4.1.

46 ENISA (2025): ENISA Single Programming Document 2025-2027.

47 The respective ECA reports can be found here (in reverse chronological order): 2023, 2022, 2021, 2020, 2019, 2018, 2017, 2016, 2015, 2014, 2013, 2012, 2011, 2010, 2009, 2008, 2007, 2006, and 2005.

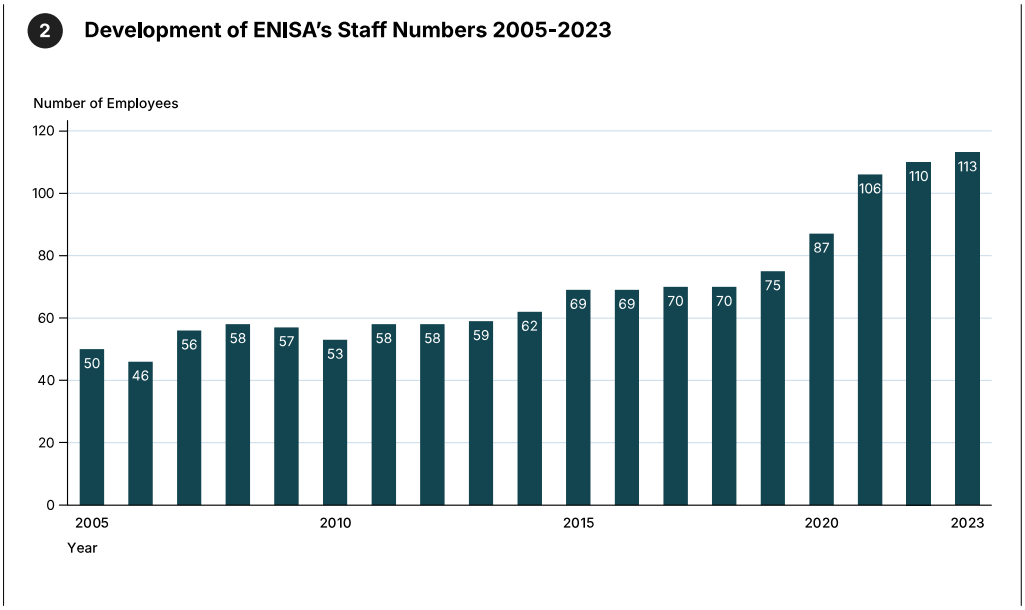

Figure 2: Development of ENISA's staff numbers 2005–2023

These numbers translate to a 126% increase in staff and a 598% increase in budget (including the additional money granted to ENISA for implementation of the Cybersecurity Support Action) between the years 2005 and 2023. When deducting additional contributions emanating from the Cybersecurity Support Action, ENISA's budget increased by 360% when compared to the year 2005 (see Figure 3).

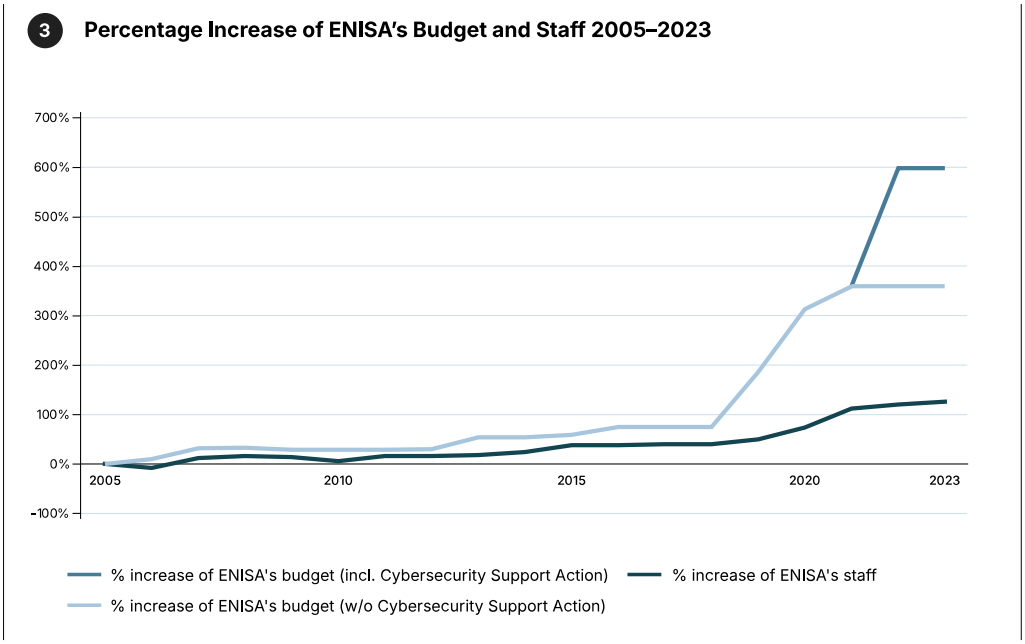

Figure 3: Percentage increase of ENISA's budget and staff 2005–2023

Challenges

This chapter outlines six key challenges facing ENISA in the fulfillment of its purpose based on various observations. These challenges are deeply interconnected, mutually reinforcing, and have a significant cumulative impact on ENISA's capacity to carry out its mandated tasks, which ultimately affects its contribution to make the European Union more cybersecure. As each challenge brings its own set of issues shaping ENISA's ability to fulfill its purpose, every section concludes with a paragraph outlining the implications for ENISA's operations and the EU cybersecurity policy ecosystem as a whole.

Challenge 1: ENISA operates within a complex, heterogeneous environment

ENISA operates in a complex and demanding environment, making its role and the place it occupies within the EU cybersecurity policy ecosystem challenging from the outset. Three observations highlight challenges pertaining to ENISA's operating environment:

Observation 1: ENISA's role and sphere of influence are contested

ENISA's mandate spans a wide range of issue areas, including awareness-raising, research, certification, and policy development (for a comprehensive overview see Section 3.3). In addition to substantial overlaps with other actors at both the EU[48] and Member State levels undertaking similar tasks, ENISA's role is being contested by the establishment of new actors at the EU level operating in areas intersecting with the agency's mandate. The most recent example of such an occurrence is the set-up of the so-called Cyber Situation and Analysis Centre housed within DG CONNECT's Cyber Coordination Task Force, to which ENISA also contributes.[49]

48 For a comprehensive overview of EU actors involved in EU cybersecurity policy, see Christina Rupp (2024): Navigating the EU Cybersecurity Policy Ecosystem, interface. For example, ENISA's work on situational awareness intersects with entities such as CERT-EU, INTCEN including the Single Intelligence Analysis Capacity (SIAC), the Cyber Coordination Task Force, and Member States CSIRTs. However, for example, ENISA's 2024 State of the Union report pointed to the fact that "a common, real-time picture encompassing all MSs and covering all aspects of situational awareness" would still be lacking to date, ENISA (2024): 2024 Report on the State of the Cybersecurity in the Union. CERT-EU and ENISA engage in a structured cooperation (ENISA (n.d.): Cooperation with CERT-EU). Moreover, ENISA's involvement in cybersecurity research and skills-related activities overlaps with the mandate of the ECCC and its network of National Coordination Centres (NCCs), the Commission-led Cybersecurity Skills Academy, and the work of research and education authorities at the Member State level. For example, in its conclusions on ENISA, the Council also "acknowledge[d] that both ENISA and the ECCC are mandated to promote skills across the Union" (Council of the EU (2024): Council conclusions on ENISA, 16527/24).

49 For further information on the Cyber Situation and Analysis Centre see, for example, European Commission (2022): Call for

In this respect, in its conclusions on ENISA, the Council of the EU also specifically invited the European Commission to "streamline the tasks of the Cyber Situation and Analysis Centre of the Commission and ENISA's related tasks."[50] Another very prominent example is the set-up of the European Cybersecurity Competence Centre (ECCC) in Bucharest, agreed upon in 2021,[51] which has assumed tasks relating to, for instance, research and skills – tasks that ENISA is also mandated to undertake.

In both instances, it is not clear what conceptual basis, for example, along the lines of strategic/operational/tactical/reflective tasks, underlies the distribution of responsibilities between ENISA, the Cyber Situation and Analysis Centre, and the ECCC. Therefore, the establishment of these actors raises the question of why the sought capacities and tasks – encompassing elements as stipulated in ENISA's mandate – were not housed or built up within ENISA itself as a strategic mid- to long-term effort, which would have supported the co-legislators' original ambition of the agency being a "centre of expertise on cybersecurity" (Art. 4(1) CSA). From a systemic and institutional perspective, this diversification in actors also further contributes to a diversification of the EU cybersecurity policy ecosystem (sometimes also labelled as a "galaxy"[52]).

Observation 2: ENISA operates in an environment with varied maturity and capability levels

ENISA's room for maneuver is further challenged by the fact that different levels of cybersecurity maturity and capabilities persist in Member States, EU entities, and sectors. Already within Member States, there is significant variation in terms of cybersecurity readiness. While noting the limitations to indexes seeking to compare national approaches, a look at the International Telecommunications Union's 2024 Global Cybersecurity Index reveals diverse levels of cybersecurity maturity in the Union. Whereas the capacities of fifteen EU Member States are considered "role-modelling," ten other Member States find themselves in the "advancing" category, and two in the "establishing" tier.[53] This variety in Member State cybersecurity maturity corresponds with the European Commission's assessment on

tenders CNECT/2022/OP/0088 - Bespoke service to support the cyber situation and analysis centre for the European Commission, Leonardo (2023): First Pan-European Cyber Analysis Centre Now Operational and European Commission (2025): Security analyst: Cyber and hybrid threats in DG Connect - European Commission.

50 Council of the EU (2024): Council conclusions on ENISA, 16527/24.

51 Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, 2021/887.

52 European Court of Auditors (2023): Opinion 02/2023 concerning the proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

53 International Telecommunications Union (2024): Global Cybersecurity Index 2024. The EU's candidate countries also reflect diverse levels of maturity, ranging from "evolving" (Bosnia and Herzegovina) to "role-modelling" (Serbia and Türkiye). As another example, ENISA's 2024 report on the state of cybersecurity also comes to the conclusion that the average maturity of CSIRTs in the Union is low, ENISA (2024): 2024 Report on the State of the Cybersecurity in the Union.

the state of "cyber preparedness" in EUIBAs.[54] The disparity is also mirrored at the sectoral level: Whereas sectors like finance and energy often exhibit (more) advanced cybersecurity levels, less resourced sectors, such as the rail or health sector, lag behind and display moderate or low maturity levels.[55] In addition, capacities are spread heterogeneously among EU citizenry, which is another target group according to ENISA's mandate.[56] For a supranational organization like ENISA, this poses a challenge, as it must tailor its outputs to diverse, distinct environments while still adding value to each. By way of a concrete example, the cybersecurity agency of a well-resourced EU Member State may be less dependent on ENISA's support, whereas others with lower cybersecurity maturity may approach ENISA with a whole different set of expectations, for example, relating to capacity-building.

Observation 3: ENISA must add value to differing national implementations

Third, ENISA faces significant heterogeneity in how Member States implement (EU) cybersecurity policies within their jurisdictions. This variability in initial policy foundations and overall approaches to cybersecurity manifests in several areas, including, for instance, cybersecurity certification[57] and market supervision.[58] In this respect, ENISA's report on the state of cybersecurity in the Union highlights divergences among Member States pertaining, inter alia, to "domains related to policy implementation, in particular with regards to vulnerability disclosure and supervisory measures for essential and important entities, as well as R&D and education" and "monitoring frequency" relating to Member States' "cybersecurity threat level."[59]

As a specific example, Member States differ in the importance they attach to sectoral versus central responsibility at the national level, as exemplified by the competent authorities designated by EU Member States pursuant to the first NIS Directive. While one entity assumes the role as the competent authority for all "operators of essential services" and "digital service providers" in the majority of Member States, others have from two up to seven entities assuming this role:[60]

54 European Commission (2022): Replies of the European Commission to the European Court of Auditors' Special Report 'Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats'.

55 ENISA (2024): 2024 Report on the State of the Cybersecurity in the Union and Kevin Eiden, James Kaplan, Bartlomiej Kazimierski, Charlie Lewis, and Kevin Telford (2021): Organizational cyber maturity: A survey of industries, McKinsey & Company.

56 In this respect, ENISA's 2024 State of the Union Report notes that "half of EU citizens lack the digital skills needed to fully participate in society, hindering their access to online services," ENISA (2024): 2024 Report on the State of the Cybersecurity in the Union.

57 For example, with respect to national cybersecurity certification systems, some EU Member States primarily focus on high-assurance certifications, while others have extensive, more comprehensive systems in place.

58 For example, some Member States still find themselves in the process of building up market supervision structures and procedures in the first place, whereas market supervision is already a well-established practice for others.

59 ENISA (2024): 2024 Report on the State of the Cybersecurity in the Union.

60 European Commission (n.d.): NIS Cooperation Group.

1	2	5	6	7
Belgium Cyprus Czechia Estonia France Germany Greece Ireland Lithuania Malta Portugal Romania Slovakia Slovenia	Austria Hungary Luxemburg Spain	Bulgaria Italy Netherlands	Latvia Sweden	Croatia Denmark Finland Poland
14 Member States	4 Member States	3 Member States	2 Member States	4 Member States

Table 1: Number of competent authorities for all operators of essential services and digital service providers designated pursuant to the first NIS Directive across Member States

Implications

The lack of a clear demarcation of ENISA's role, competences, and relationship with other entities at both the EU and the Member State levels can pose notable consequences. Without a designated body to coordinate cybersecurity at the EU level, this ambiguity – at worst, contributing to confusion and fragmentation – can result in inefficiencies and duplicated efforts. For ENISA, it increases the need for coordination with other actors, which may hinder its ability to develop specialized expertise.[61] The diverse approaches to cybersecurity policy implementation and the varying maturity levels across Member States, EUIBAs, and sectors present challenges to implementing a uniform, horizontal framework. Given its broad mandate but limited resources (see also Section 4.6), ENISA must maintain a deep understanding of national and sectoral contexts[62] to address the distinct yet

61 This lack of focus was, for example, addressed by Czechia's National Cyber and Information Security Agency (NUKIB) in its publicized response to the Commission's ENISA evaluation, stating that ENISA's publications "tend to be excessively long and too descriptive" and a corresponding wish that ENISA would become "more selective in terms of document production and their overall length, paying higher attention to the current topics and policy questions raised by the Member States," National Cyber and Information Security Agency of the Czech Republic (2023): Response to evaluation of ENISA by European Commission.

62 With respect to sectoral engagements, ENISA settled for a layered engagement with different sectors in 2023 within its NIS strategy (not publicly available) by developing "targeted packages/bundles of services" and prioritizing those sectors that require particular guidance and assistance. The agency distinguishes between four distinct objectives: (1) 'build' as "immature sectors that need to improve" (health and rail sectors), (2) 'sustain' covering "mature sectors that need continued support and ENISA leadership" (telecoms, digital infrastructure, trust, energy sectors), (3) 'involve' targeting "mature sectors where sectoral stakeholders take the lead" (finance, aviation, and space sectors), and (4) 'prepare' including "new NIS sectors that may require ENISA's support in the future" (gas and water sectors as well as public administrations), ENISA (2024): ENISA Consolidated Annual Activity Report 2023. The agency's 2025 work program notes that ENISA would support working groups comprising representatives from Member State authorities for every listed sector in the framework of activity 2 (ENISA (2025): Single

interconnected priorities of multiple stakeholders. These peculiarities can pose a challenge to ENISA's activities, as the agency must account for these specificities in its work to have impact, yet it must find a way to do so in a resource-preserving way while also ensuring the highest possible level of interoperability.

Challenge 2: ENISA's expansion of tasks results in mounting expectations from a steadily increasing number of actors

In recent years, the EU's regulatory scope covering cybersecurity matters has expanded significantly. Over time, the EU's regulatory efforts have transitioned from a 'light touch' approach to a more robust framework. This has resulted in a growing variety and number of entities, including, for instance, Member State entities, EU bodies, and other actors like energy network operators and domain name system service providers now being subject to elevated cybersecurity obligations and respective mechanisms for enforcement across the Union. These developments have also accelerated ENISA's relevance and the agency has gained prominence, as evidenced by the increase in mentions of ENISA in EU documents in percentage terms within the last two decades (see Figure 6 below).[63]

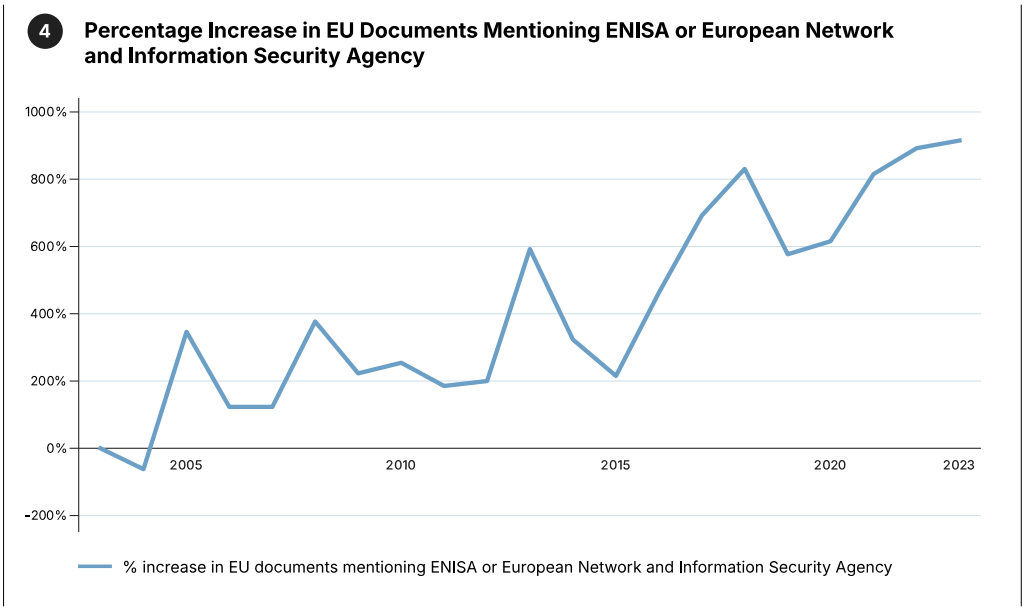

Figure 4: Percentage increase in EU documents mentioning ENISA or European

Programming Document 2025-2027).

63 The following number of results for documents mentioning ENISA apply to exemplary years: 58 (2005), 46 (2010), 41 (2015), 93 (2020), and 132 (2023).

Network and Information Security Agency[64]

The documents mentioning ENISA often also specifically confer tasks to the agency. Many of these tasks stem from legislation adopted within recent years, emphasizing the gradual expansion of ENISA's tasks among a wide variety of actors: EUIBAs and EU-internal coordination bodies, Union-level cooperation and EU–Member State-coordination bodies, Member State entities, and non-state stakeholders and bodies with stakeholder involvement. With more entities and ICT products falling within the scope of EU cybersecurity legislation, a continuously growing number of actors with varied portfolios has – and more openly expresses – expectations regarding ENISA.

A few observations underscore this development:

Observation 1: ENISA must cater to a comprehensive actor network

As Table 2 below shows (for a more detailed version see Annex II, Section 6.2), EU legislation provides for a diverse and expanding network of relationships involving ENISA by outlining interactions and relationships with various specific actors. The designated relationships are often bidirectional since ENISA acts, for instance, both as a provider of assistance as well as a recipient of information from actors, such as Member State entities.

Actor Group	Actors (in alphabetical order)	
EU Institutions, Bodies, and Agencies and EU-internal coordination bodies	EU Institutions	• European Central Bank (ECB) • European Commission
	EU Bodies	European Data Protection Supervisor (EDPS)
	EU Agencies	• European Cybersecurity Competence Centre (ECCC) • European Supervisory Authorities (ESAs) • European Union Agency for Law Enforcement Cooperation (Europol) & European Cybercrime Centre (EC3) • European Union Agency for the Cooperation of Energy Regulators (ACER) • European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)

64 Based on results for "ENISA" or "European Network and Information Security Agency" excluding corrigenda in EUR-Lex.

	EU Interinstitutional Services	Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU)
	EU-internal Coordination Bodies	Interinstitutional Cybersecurity Board (IICB)
Union-level cooperation and EU–Member State coordination bodies	• CSIRTs Network • European Cybersecurity Certification Group (ECCG) • European cyber crisis liaison organisation network (EU-CyCLONe) • European Data Innovation Board • European Data Protection Board • European Digital Identity Cooperation Group • Interoperable Europe Board • NIS Cooperation Group • Oversight Forum	
Member States	• Certification body • Cyber Resilience Act designated market surveillance authorities • Electronic Communications Code competent authorities • National CSIRTs • National cybersecurity certification authority • Network Code competent authorities • NIS 2 cyber crisis management authorities and CSIRTs • Single Point of Contact (SPOC) • Single point of contact for trust services, European Digital Identity Wallets, and notified electronic identification schemes	
Non-state stakeholders and bodies with stakeholder involvement	• AI Act Advisory Forum • Certification body • "Citizens, organisations and businesses (across the Union)" • ENTSO for Electricity and the EU DSO entity • High- and critical-impact entities • Manufacturers • Natural or legal persons • Public • Sectoral entities • Stakeholder Cybersecurity Certification Group (SCCG) • Transmission system operators (TSOs)	

Table 2: Overview of ENISA's actor network as derived from EU legislation (for more details on their legal bases, see Annex II, Section 6.2)[65]

65 This table does not cover EU policies of a non-regulatory nature and does not account for tasks assigned not ENISA not specifying a particular actor within the alluded actor groups.

Observation 2: ENISA maintains a wide web of relationships

ENISA's actor network is further expanded when accounting for relationships specified in policy documents and interactions otherwise alluded to in ENISA's annual activity report or other publicly available sources, such as the agency's website. Overall, their relationship encompasses a very wide scope, comprising, for example, cooperation in the implementation of joint activities and events, or the issuance of joint publications.

Actor Group	Actors (in alphabetical order)	
EU Institutions, Bodies, and Agencies and EU-internal coordination bodies	EU Institutions	• Horizontal Working Party on Cyber Issues (HWPCI) [66]
	EU Bodies	• European External Action Service (EEAS) [67] including European Security and Defence College (ESDC) [68]
	EU Agencies	• Agency for Support for BEREC (BEREC Office) [69] • European Defence Agency (EDA) [70] • European Maritime Safety Agency (EMSA) [71] • European Supervisory Authorities (ESAs, European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA)) [72] • European Union Agency for Fundamental Rights (FRA) [73] • European Union Agency for Law Enforcement Cooperation (Europol) [74] including European Cybercrime Centre (EC3) [75] • European Union Agency for Law Enforcement Training (CEPOL) [76] • European Union Agency for Railways (ERA) [77] • European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) [78] • European Union Agency for the Space Programme (EUSPA) [79] • European Union Aviation Safety Agency (EASA) [80]
	EU-internal Coordination Bodies	• EU Agencies Network (EUAN) [81]
European organizations, that are not EUIBAs	• European Standards Organisations (ESOs, including European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) and European Telecommunications Standards Institute (ETSI)) [82] • European Organisation for the Safety of Air Navigation (Eurocontrol) [83]	

Union-level Cooperation and EU–Member State coordination bodies	• European Competent Authorities for Secure Electronic Communications Expert Group (ECASEC) [84] • European Competent Authorities for Trust Services Expert Group (ECATS) [85] • Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) including Cyber Information and Intelligence Sharing Initiative (CIISI-EU)

Non-state stakeholders and bodies with stakeholder involvement	• ENISA Ad Hoc Working Groups [86] (it is sometimes not entirely clear which of them are still active)
	  • Ad Hoc Working Group on EU Cybersecurity Market
	  • Ad Hoc Working Group on EU Digital Identity Wallets Cybersecurity Certification [87]
	  • Ad hoc Working Group on National Risk Management Preparedness
	  • Ad-Hoc Working Group on 5G Cybersecurity Certification [88]
	  • Ad-Hoc Working Group on Artificial Intelligence Cybersecurity [89]
	  • Ad-Hoc Working Group on Awareness Raising
	  • Ad-hoc Working Group on Cloud Services
	  • Ad-Hoc Working Group on Cyber Threat Landscapes
	  • Ad-Hoc Working Group on Data Protection Engineering
	  • Ad-Hoc Working Group on Enterprise Security
	  • Ad-Hoc Working Group on Foresight On Emerging And Future Cybersecurity Challenges
	  • Ad-hoc Working Group on Risk Assessment and Risk Management
	  • Ad-Hoc Working Group on the European Cybersecurity Skills Framework (2023-2025) [90]
	  • Ad-hoc Working Group Transposition of the SOGIS-MRA certification framework
	• Information Sharing & Analysis Centers (ISACs) [91]

Other	• Forum of Incident Response and Security Teams (FIRST) [92] • International Organization for Standardization (ISO) [93]

66 Council of the EU/European Council (2024): Horizontal Working Party on Cyber Issues (Cyber).
67 ENISA (2022): Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape.
68 European Security and Defence College (n.d.): Network Members and European Security and Defence College (n.d.): EAB.Cyber.
69 Body of European Regulators for Electronic Communications (2021): BEREC's Medium Term Strategy for relations with other institutions 2022-2025.
70 European Defence Agency (n.d.): Cyber and European Defence Agency (2018): Memorandum of Understanding between ENISA, EDA, EC3, and CERT-EU.
71 ENISA (2022): Maritime Sector Sails through rough 'Cybersecurity' Seas.
72 ENISA (2024): ESAs and ENISA sign a Memorandum of Understanding to strengthen cooperation and information exchange.
73 European Union Agency for Fundamental Rights (2024): Consolidated Annual Activity Report of the European Union Agency for Fundamental Rights 2023.
74 Europol (2014): Agreement on Strategic Co-operation between the European Agency for Network and Information Security and the European Police Office and ENISA (2024): Joint Statement on Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities.
75 ENISA (2021): CSIRT - Law Enforcement Cooperation Workshop - 10 Years of Joint Efforts against Cybercrime.
76 CEPOL (2019): CEPOL high-level meetings in Athens.
77 European Union Agency for Railways (2024): 4th ERA-ENISA Conference on Cybersecurity in Railways.
78 ENISA (2021): ENISA and eu-LISA – Cooperation for a More Digitally Resilient Europe.
79 European Union Agency for the Space Programme (2023): Securing the EU Space Programme starts with EUSPA.
80 ENISA (n.d.): Transport.
81 EU Agencies Network (2023): 2024-2025 Work Programme.
82 ENISA (2024): 9th Cybersecurity Standardisation Conference and CENELEC (n.d.): European Partners.
83 Eurocontrol (2023): ATM: navigating the challenging cybersecurity landscape.

	• International Telecommunication Union (ITU)[94]

Table 3: Expansion of ENISA's actor network accounting for other sources

Observation 3: ENISA faces rising expectations from various actor groups

With Tables 2 and 3 together comprising (at least parts of) ENISA's complex actor network, expectations are not only implicitly held by this network but also increasingly expressed explicitly. One can distill several lines of implicit and explicit sets of expectations from the responses to the ENISA evaluation – most of which stem from business associations and private sector enterprises – as well as the recent Council conclusions on ENISA, and other sources. The following seven examples are non-exhaustive but provide a good overview over some of the expectations facing ENISA:

1. **ENISA should follow through more thoroughly on specific stipulations in its mandate**: For example, in 2022, the ECA noted that ENISA lacks comprehensive insight into the specific practices of individual EUIBAs with respect to their vulnerability disclosure policies and does not provide support in creating or executing these policies – a task foreseen in ENISA's mandate as stipulated in the CSA.[95] In their conclusions on ENISA, Member States have also voiced a desire for ENISA to "share and actively promote technical guidance and best practices in a regular and structured manner assisting the Member States in implementing cybersecurity policy and legislations."[96]
2. **ENISA should provide additional guidance, education, and/or expertise**: For instance, Digital Europe, advocated that "ENISA should deepen its sector-specific expertise to provide tailored guidance and support to critical sectors."[97] Another private sector stakeholder, a US-based company, called for support by ENISA in "navigat[ing] the EU cybersecurity legislative landscape" through the development of "educational tools for companies to help them prepare for future legislation."[98]

84 ENISA (n.d.): Telecom sector and Digital Infrastructure and ENISA (2021): EU Electronic Communications Security Authorities Discussion on Incident reports and Policy.
85 ENISA (n.d.): ECATS EG.
86 In their response to the ENISA evaluation, Danish authorities mentioned that they "see limited benefits from the ones [ad hoc working groups] in which we have been engaged, not least given the challenges pointed out in our input above regarding the organizational structure, working practices and performance of ENISA", Danish Ministry of Digital Government and Gender Equality & Danish Ministry of Defence (2023): Response to evaluation of ENISA by European Commission.
87 ENISA (2024): Call for Experts: Join the ENISA Ad Hoc Working Group on EU Digital Identity Wallets Cybersecurity Certification.
88 ENISA (2021): Call 01/21 - 5G Cybersecurity Certification.
89 ENISA (2020): Call for Expression of Interest: Experts Group in Artificial Intelligence Cybersecurity.
90 ENISA (n.d.): Ad-Hoc Working Group on the European Cybersecurity Skills Framework (2023-2025).
91 ENISA (2022): ENISA Supports the Cooperation among Sectorial Information Sharing & Analysis Centers (ISACs) and EE-ISAC (n.d.): Who We Are.
92 FIRST (n.d.): FIRST Liaison Members.
93 ISO (n.d.): Organizations in cooperation with ISO and ISO/IEC JTC 1 (n.d.): Partner Organizations.
94 International Telecommunications Union (n.d.): European Union Agency for Network and Information Security.
95 European Court of Auditors (2022): Cybersecurity of EU institutions, bodies and agencies. Level of preparedness overall not commensurate with the threats.
96 Council of the EU (2024): Council conclusions on ENISA, 16527/24.
97 DIGITALEUROPE (2023): Response to evaluation of ENISA by European Commission: Adapting ENISA's mandate and collaboration in a changing cyber landscape.
98 Workday (2023): Comments on the European Commission's call for evidence on the evaluation of ENISA and the European

3. **ENISA should enhance opportunities for collaboration with the private sector, stakeholders, and public authorities**: For example, Microsoft advocated for the establishment of a dedicated unit for a more structured engagement with the private sector,[99] whereas Digital Europe underscored the need to enhance "collaboration with sector-specific authorities and organisations, such as ISACs [Information Sharing and Analysis Centers]."[100] Also the Finnish IT Center for Science referred to limited engagement of ENISA at the national level with private sector stakeholders, alluding to CSIRTs as an example,[101] and the American Chamber of Commerce to the EU sought elevation of communication with ENISA from a "one-way process" to a two-way interaction.[102] The European Consumer Organization highlighted the need for increased ENISA activities dedicated to outreach to "fully deliver on its [the agency's] mandate of developing and implementing EU policies on cybersecurity, particularly in relation to consumers."[103] In its contribution, Microsoft also outlined the perceived benefits of elevating and expanding the agency's relationship with each EU Member State as well as EU institutions, specifically the Council and the European Parliament.[104] A public transport sector entity emphasized the limited visibility and knowledge of ENISA in the sector.[105] For example, in its conclusions on ENISA, the Council called on the agency "to consider ways to enhance the collaboration between ENISA and European standardisation bodies" and encouraged the agency "to bolster cooperation with the private sector."[106]
4. **ENISA should be conferred additional tasks**: For instance, the REWIRE project recommends integration of the "ownership and maintenance of the ECSF [European Cybersecurity Skills Framework]" as part of the agency's mandate,[107] while ISACA has made the case for adding the development of a certification scheme for cybersecurity skills to ENISA's tasks.[108]
5. **ENISA should expand the list of actors it seeks to target with its outputs**: For example, the International Association of Public Transport implicitly called for elevated consideration of the specificities and concerns of the public transport sector throughout ENISA's work relating to transport.[109] The City of Stockholm advocated for a more comprehensive translation of ENISA's outputs, such as training materials, to enhance the agency's value added at the local, municipal level.[110]
6. **ENISA should pay increased attention to developments relating to emerging technologies**: For instance, the Information Technology Industry Council (ITI), Kaspersky, and Microsoft called for the consideration of emerging technologies as part of its mandate.[111] In this respect, ITI and Microsoft specifically alluded to AI and

Cybersecurity Certification Framework.

99 Microsoft (2023): Microsoft Contribution to Call for Evidence. ENISA & the European Cybersecurity Certification Framework. The call for a dedicated unit was also referenced in the American Chamber of Commerce to the EU's contribution.

100 DIGITALEUROPE (2023): Response to evaluation of ENISA by European Commission: Adapting ENISA's mandate and collaboration in a changing cyber landscape.

101 CSC – IT Center for Science (2023): Response to evaluation of ENISA by European Commission.

102 American Chamber of Commerce to the EU (2023): Consultation response: Evaluation of ENISA and the European Cybersecurity Certification Framework.

103 BEUC - The European Consumer Organisation (2023): Response to evaluation of ENISA by European Commission.

104 Microsoft (2023): Microsoft Contribution to Call for Evidence. ENISA & the European Cybersecurity Certification Framework.

105 International Association of Public Transport (2023): Response to evaluation of ENISA by European Commission.

106 Council of the EU (2024): Council conclusions on ENISA, 16527/24.

107 REWIRE project (2023): Response to evaluation of ENISA by European Commission.

108 ISACA (2023): ISACA response: European Commission's evaluation of the European Union Agency for Cybersecurity and EU cybersecurity certification framework.

109 International Association of Public Transport (2023): Response to evaluation of ENISA by European Commission.

110 Stockholms stad (2023): Response to evaluation of ENISA by European Commission.

111 Information Technology Industry Council (2023): ITI Response to the Consultation on the European Union Agency for Cybersecurity and EU cybersecurity certification framework, Kaspersky (2023): Response to evaluation of ENISA by European Commission, and Microsoft (2023): Microsoft Contribution to Call for Evidence. ENISA & the European Cybersecurity Certification Framework.

quantum computing.

7. **ENISA should increase its international engagement** (see also Section 4.5): Not surprisingly, stakeholders operating worldwide or headquartered outside of EU Member State jurisdictions emphasize the importance of giving a boost to ENISA's international endeavors.[112] For example, in this respect, the ITI mentioned the goals of ENISA being a regular participant in the EU-US Cyber Dialogue and cooperating with the Organisation for Economic Co-operation and Development (OECD),[113] and the American Chamber of Commerce to the EU alluded to "NATO partners from outside the EU."[114]

In summary, the following actor groups have publicly placed expectations on ENISA:

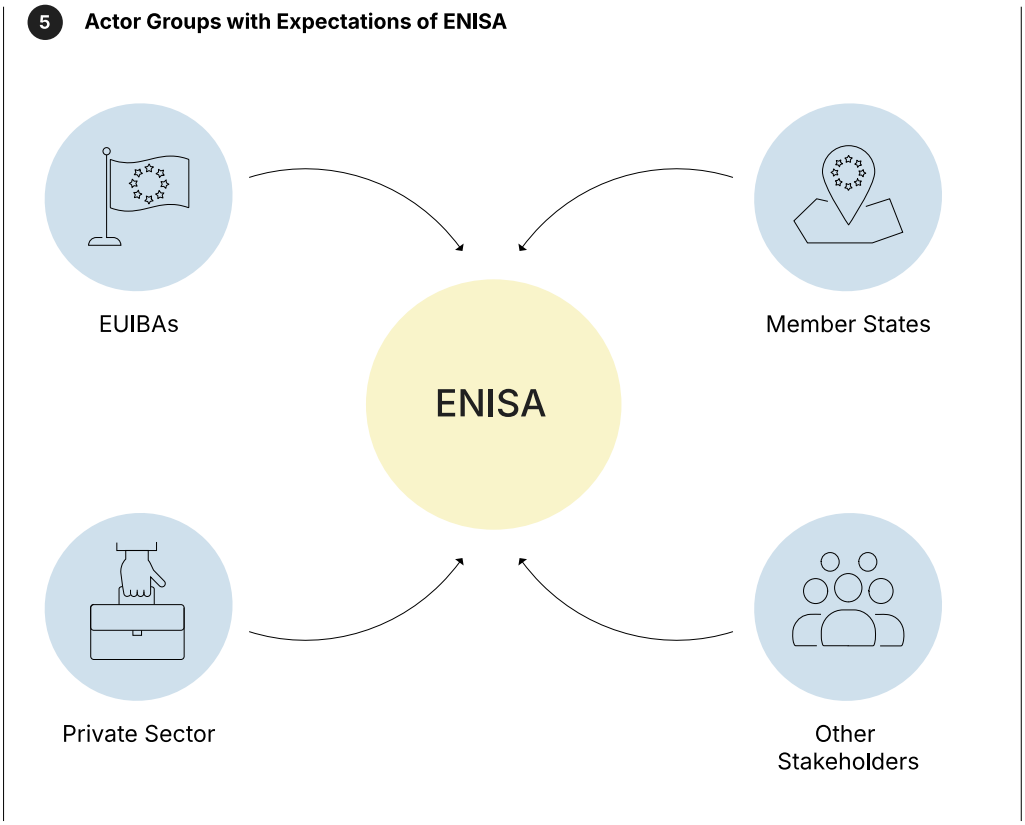

Figure 5: Actor groups with expectations for ENISA

112 Microsoft (2023): Microsoft Contribution to Call for Evidence. ENISA & the European Cybersecurity Certification Framework, Information Technology Industry Council (2023): ITI Response to the Consultation on the European Union Agency for Cybersecurity and EU cybersecurity certification framework, Kaspersky (2023): Response to evaluation of ENISA by European Commission, and American Chamber of Commerce to the EU (2023): Consultation response: Evaluation of ENISA and the European Cybersecurity Certification Framework.

113 Information Technology Industry Council (2023): ITI Response to the Consultation on the European Union Agency for Cybersecurity and EU cybersecurity certification framework.

114 American Chamber of Commerce to the EU (2023): Consultation response: Evaluation of ENISA and the European Cybersecurity Certification Framework.

Implications

Meeting the expectations of these various stakeholders requires substantial effort and resources from ENISA. Given its limited financial and human resources (see further Section 4.6), effectively managing these expectations demands a strategic approach and prioritization by the agency and/or higher political levels. The responses to the ENISA evaluation exemplify that these efforts have been insufficient to date. This results in an important challenge for ENISA: If the agency is expected to provide equal or substantial support to all actors in the EU cybersecurity ecosystem, its limited capacity will most likely prevent it from offering comprehensive assistance to any one group and from fully leveraging its unique position.

Challenge 3: ENISA's activities extend beyond exclusively internal market–driven objectives as the agency's operational footprint continues to grow

Building upon the principle of conferral, the EU needs competence – exclusively or shared with the Member States – to take action in a particular policy field (Art. 5 Treaty on European Union (TEU)). In accordance, any competencies not specified in EU primary law "remain with the Member States" (Art. 5(2) TEU). Hence, for example, EU Member States retain exclusive competence over national security (Art. 4(2) TEU), with some countries being resistant to any EU involvement in this sensitive area.[115] Therefore, EU cybersecurity legislation often includes disclaimers to clarify that these measures do not infringe upon Member States' competence in matters of public security, defense, national security, or state activities in criminal law, as illustrated, for instance, in Art. 1(2) of the CSA,[116] thereby also specifying red lines for ENISA's activities. The CSA draws on EU competences in relation to the internal market as the legal basis for the agency's establishment by referencing Art. 114 TFEU and specifying "ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and

115 Since this is ultimately an issue of power, the complexities of navigating the issue of national security in an EU cybersecurity policy context are exemplified by the proposal for the establishment of a Joint Cyber Unit (JCU), which has resulted in considerable backlash. Even if some elements of the proposal of a JCU made their reappearance through the Cyber Solidarity Act, it is still an emblematic example as some Member States perceived it to be too close to national security, which has contributed to the political death of the initiative. See, for instance, Alberto Di Felice (2023): Can the Cyber Solidarity Act Vindicate the Joint Cyber Unit?.

116 "This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law," Art. 1(2) CSA.

trust within the Union" (Art. 1(1) CSA) as the agency's objective. Also, during a 2020 event, ENISA's Executive Director Juhan Lepassaar referred to ENISA as an "internal market agency."[117]

Given the cross-cutting nature of cybersecurity, there are, however, inevitable interlinkages between cyber and national security. While the internal market remains central to ENISA's mandate – for instance, in relation to the implementation of the NIS 2 Directive – the agency's growing operational footprint indicates that ENISA is de facto assuming a broader role going beyond purely internal market–driven considerations or entirely economy-related goals such as ensuring the cohesion and prosperity of the EU as "an area without internal frontiers [... permitting] the free movement of goods, persons, services and capital" (Art. 26(2) TFEU). The 2019 CSA also includes operational cooperation as one of the eight pillars of ENISA's work, mandating ENISA, inter alia, to regularly organize exercises (Art. 7(5) CSA)[118] and contribute to the "develop[ment of] a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity," for example, by "facilitating [upon request] the technical handling of such incidents or crises, including, in particular, by supporting the voluntary sharing of technical solutions between Member States" (Art. 7(7), point (c)) CSA).

A few concrete examples in the areas of incident and crisis management, situational awareness, and operational coordination illustrate this development:

1. First, ENISA plays a considerable role in providing the secretariat and supporting the work of the **CSIRTs Network**[119] and the **European Cyber Crisis Liaison Organisation Network** (EU-CyCLONe).[120]
2. Second, the **Blueprint on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises** – as well as the European Commission's 2025 update proposal[121]

117 Institute of International and European Affairs (2020): Juhan Lepassaar - The EU Cyber Crisis Cooperation Framework – An ENISA Perspective, YouTube, 48:20. On a historical note, the internal market legal basis for establishing ENISA has been upheld by the European Court of Justice, to the extent, however, that "the Community body thus established provides services to national authorities and/or operators which affect the homogenous implementation" of internal market legislation, European Court of Justice (2006): Judgement of 2 May 2006, Case C-217/04. The TFEU defines the EU's internal market as "an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties" (Art. 26(2) TFEU).

118 See, for example, ENISA (n.d.): Trainings and exercises.

119 For instance, ENISA supports Member States' operational cooperation in the CSIRTs Network framework (in structured cooperation with CERT-EU) by "advising on how to improve their capabilities to prevent, detect and respond to incidents and, at the request of one or more Member States, providing advice in relation to a specific cyber threat" (Art. 7(4) CSA) and contributes to the "develop[ment of] a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity" by "ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs network and the technical and political decision-makers at Union level" (Art. 7(7), point (b) CSA). The NIS 2 Directive also tasks ENISA with briefing the CSIRTs Network every six months on "findings on notifications received" (Art. 23(9) NIS 2 Directive).

120 Complementary to its secretariat functions, the NIS 2 Directive tasks ENISA with "support[ing] the secure exchange of information" (Art. 16(2) NIS 2 Directive) and providing the "necessary tools to support cooperation between Member States ensuring secure exchange of information" (Art. 16(2) NIS 2 Directive) in the context of EU-CyCLONe. The CRA provides for the opportunity for ENISA to submit to EU-CyCLONe "information notified pursuant to Article 14(1) and (3) and Article 15(1) and (2) if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level" (Art. 17(1) CRA).

121 European Commission (2025): Cyber Blueprint - Draft Council Recommendation.

– foresees the involvement of ENISA. ENISA is also part of the EU's so-called **interinstitutional Cyber Crisis Task Force**.[122]

3. Also, the 2017 and 2023 implementing guidelines on the EU's **Cyber Diplomacy Toolbox** refer to contributions by ENISA, for instance, in the area of situational awareness.[123] Throughout recent years, ENISA was also frequently present when the Horizontal Working Party on Cyber Issues (HWPCI) discussed developments relating to the Cyber Diplomacy Toolbox.[124]
4. Further examples of ENISA's increased engagement in operational activities are the issuance of **EU Joint Cyber Assessment Reports** (EU-JCAR) together with CERT-EU and Europol as well as a one-time alert published jointly with CERT-EU in February 2023 highlighting activities by various Chinese advanced persistent threat (APT) groups.[125]

Implications

Despite the limitations on EU action in the area of national security, these activities – along with the overall evolution of the EU's cybersecurity acquis – demonstrate that cybersecurity has increasingly become an area where national and EU-level security concerns intersect. ENISA Executive Director Lepasaar has also emphasized that security and cybersecurity are increasingly being considered together,[126] and ENISA's growing operational footprint exemplifies this shift. At the same time, there is continued interest from Member States in ENISA activities relating to operational cooperation. In their conclusions on ENISA, the Council invited the European Commission "to examine and further strengthen ENISA's role in supporting operational cooperation at the EU level [...], taking into account Member States' competences in this field."[127] However, discussions around initiatives such as the CSOA and the Joint Cyber Unit have highlighted the ongoing challenge of striking a balance between EU-level coordination in operational matters and national sovereignty–related concerns. Therefore, looking ahead, a key question will be how "operational" should be defined in the context of ENISA's mandate. Should ENISA become a more operational actor itself – for example, by directly engaging with entities in Member States as envisioned, for example, by the European Commission most recently in its EU Health Action Plan (which is something that some Member States strongly oppose)? Or should ENISA limit its

122 European Commission (2017): Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises, 2017/1584 and Council of the EU (2024): Council Recommendation on a Blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance, 10653/24.

123 Council of the EU (2017): Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - approval of the final text, 13007/17 and Council of the EU (2023): Revised Implementing Guidelines of the Cyber Diplomacy Toolbox, 10289/23.

124 For example, Council of the EU General Secretariat (2024): Horizontal Working Party on Cyber Issues, Notice of Meeting and Provisional Agenda, CM 3048/24.

125 ENISA (2024): ENISA Consolidated Annual Activity Report 2023 and ENISA (2023): Sustained Activity by Threat Actors - Joint Publication.

126 "Wir erleben eine Art Neudenken der Zusammenarbeit, der Koordination zwischen den europäischen Partnern, aber auch mit unseren Verbündeten und das Zusammendenken von Sicherheit und Cybersicherheit," Johannes Steger (2024): Porträt von Juhan Lepassaar, Tagesspiegel.

127 Council of the EU (2024): Council conclusions on ENISA, 16527/24.

role to exclusively facilitating and supporting Member State–led operational activities?

Challenge 4: ENISA's purview is progressively shaped by political dynamics

ENISA Executive Director Lepassaar, has acknowledged the significant changes impacting the agency's role, stating: "For twenty years we have been watching over the cyber security of the Union, but for twenty years not many political projects happened. It was a technical debate, not a political one – that has changed considerably"[128] (author's translation). At the same time, Lepassaar emphasized ENISA's identity as a technical agency focused on drawing up plans rather than acting as an implementing authority or applying political standards.[129] While this deliberate shying away from political issues and focus on technical deliverables over the years has likely been an important factor contributing to the agency's institutionalization,[130] the reality of ENISA's increasingly politicized context has implications for the agency.

Four observations illustrate the implicit politicization of ENISA activities over recent years:

Observation 1: Cybersecurity has become more relevant to EU policy-making

The increasing prominence of cybersecurity at the EU level is evident in the significant increase in the frequency with which terms related to cyber and IT security have been mentioned in EU documents over the years. In parallel, this general evolution elevated the agency's visibility and, with the issue gaining political prominence, resulted in a gradual expansion of conferred tasks to ENISA (see also Section 4.2).

128 "Seit zwanzig Jahren wachen wir über die Cybersicherheit der Union, aber zwanzig Jahre passierten nicht viele politische Vorhaben. Es war eher eine technische Debatte, keine politische – das hat sich erheblich verändert," Johannes Steger (2024): Porträt von Juhan Lepassaar, Tagesspiegel.

129 "Wir sind eine technische Agentur, wir machen also die technische Arbeit. Wir entscheiden nicht, wir entwerfen Pläne, aber wir sind nicht die Durchführungsbehörde und legen auch keine politischen Maßstäbe an," Johannes Steger (2024): Porträt von Juhan Lepassaar, Tagesspiegel.

130 See also Myriam Dunn Cavelty and Max Smeets (2023): Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority, Journal of European Public Policy 30(7).

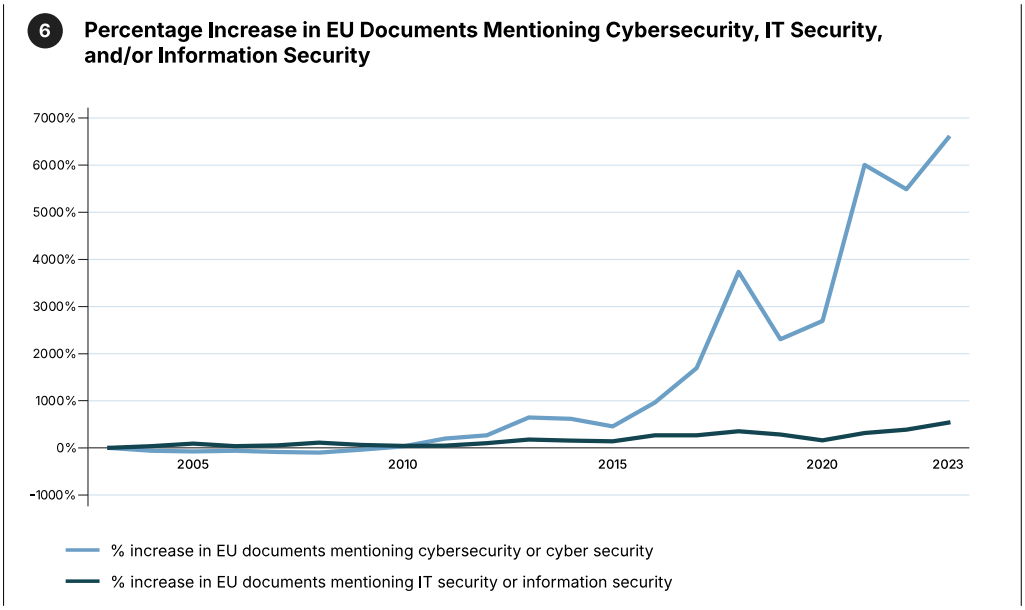

Figure 6: Percentage increase in EU documents mentioning cybersecurity, IT security, and/or information security[131]

Observation 2: ENISA is increasingly involved in policy development

In addition, ENISA not only works with outputs from the political level or builds its work upon them, but the agency is also increasingly involved or consulted in the context of policy-making. Activities relating to the development and implementation of Union policy and law also make up the first cluster of tasks assigned to ENISA (see further Art. 5 CSA). Comparing the respective passages included in ENISA's annual activity reports over the years 2017–2023 shows a gradual increase. ENISA's 2023 Annual Activity Report provides a good overview of the scope and status quo of ENISA's political engagement on various legislative files (Table 4):[132]

File	Vis-à-vis	Specification	
Cyber Resilience Act	European Commission	• "Provi[sion of] technical advice [...] on topics such as vulnerability/incident notification, scoping of critical products, EU common criteria (EUCC)	< 25 interactions with DG CONNECT and

131 Based on results for for "cyber security" or "cybersecurity" excluding corrigenda, and "information security" excluding corrigenda in EUR-Lex.
132 See also pp. 18–24, ENISA (2024): ENISA single programming document 2024-2026.

		relevance and product evaluations"	
	European Parliament	• "Provi[sion of] opinion and technical advice to [...] Members of the European Parliament (MEPs) / rapporteurs and European Parliament technical staff [...] on topics including Article 11, voluntary notification"	European Parliament
	Council of the EU	• "Provi[sion of] opinions to the HWPCI on aspects associated with the projected role of the agency in the CRA"	
Cyber Solidarity Act	Council of the EU	• HWPCI: Interaction "on topics related to the role envisaged for ENISA in the CSOA"	
	European Commission	• DG CONNECT: Analysis of "the capacity of the security operation centres (SOCs) of operators of essential services /digital service providers in the EU to provide technical advice and data"	7 "technical meetings/ workshops" with DG CONNECT and European Parliament
	European Parliament	• MEPs/rapporteurs and European Parliament technical staff: Provision of opinion and technical advice "in the preparation of the European Parliament position"	
Cybersecurity Act Amendment	European Commission & European Parliament	• "Provi[sion of] technical advice on the alignment of the definition of managed security service providers across different legislative instruments (the NIS 2, the CSOA and the CSA amendment)"	
Artificial Intelligence Act	European Commission	• "Provi[sion of] advice on cybersecurity aspects of the AI Act and by liaising with different DG Connect units on aligning market surveillance aspects for notifications and security measures and to discuss the role of ENISA in AI Office"	"Monthly interactions"

Table 4: ENISA's involvement in the development of various policy files based on its 2023 annual activity report

In this respect, ENISA also claimed success, as it underscored that its perspectives were reflected in the final text of the CRA.[133]

133 ENISA (2024): ENISA Consolidated Annual Activity Report 2023.

With the number of EU legislative acts of relevance to cybersecurity growing, ENISA is also increasingly designated to be consulted or involved in the European Commission's drafting of various non-legislative acts through the provision of advice, including, for example, the delegated or implementing acts to be adopted pursuant to the NIS 2 Directive, the Regulation on the internal markets for renewable gas, natural gas and hydrogen (2024/1789), the CRA, or the CSOA. Despite the recognition for the importance of this area of work, only a small number of ENISA staff were involved in implementing the agency's policy development activities in 2023 given resource constraints.[134] Against this backdrop, it is not surprising that ENISA, in its 2024 report on the state of cybersecurity in the Union, implicitly advocated for enhanced involvement in the development of EU policies in the context of its recommendation relating to sectoral specificities.[135] Other stakeholders have in the past also called for ENISA "to play a more prominent role in advising on planned EU legislative initiatives with cybersecurity implications."[136] In this endeavor, ENISA has the Member States on its side, as they recently called on the European Commission to "reinforce ENISA's advisory role in providing expert and evidence-based guidance and recommendations, with regard to the implementation of current and future EU legislative and non-legislative initiatives."[137]

Observation 3: ENISA's participation in HWPCI meetings has grown

Judging by the publicized agendas of the HWPCI (and its predecessor group[138]), representatives of ENISA have become more regular participants in the HWPCI over the years (see Figure 7).

134 In 2023, only 2.49 FTEs worked toward implementing the agency's policy development activity compared to 4.8 FTEs in 2022 and 4.43 FTEs in 2021, ENISA (2024): ENISA Consolidated Annual Activity Report 2023, ENISA (2023): Consolidated Annual Activity Report 2022 and ENISA (2022): Consolidated Annual Activity Report 2021. Before 2021, the annual activity reports had a single 'policy' category encompassing both policy development and policy development so the numbers cannot be compared.

135 Specifically, the agency stated that "the EU is encouraged to capitalise on ENISA's technical expertise in cybersecurity to increase the preparedness and resilience of a sector's cybersecurity and is especially advised to seek ENISA's technical evaluation of any policy initiative that could have an impact on the preparedness and resilience of a sector's cybersecurity," ENISA (2024): 2024 Report on the State of the Cybersecurity in the Union. In its 2023 Annual Activity Report, the agency similarly hinted at is ambition for increased involvement, specifically in a legislative file's early stages ("The impact of ENISA's work in policy development is multiplied when the agency is involved from the start of the policy development process"), and the Management Board appears to have endorsed this endeavor by "call[ing] on the agency to strengthen relationships with stakeholders to further support with the coherence and harmonisation of policy files before adoption" in its assessment of this report, ENISA (2024): ENISA Consolidated Annual Activity Report 2023.

136 DIGITALEUROPE (2023): Adapting ENISA's mandate and collaboration in a changing cyber landscape.

137 Council of the EU (2024): Council conclusions on ENISA, 16527/24.

138 The Friends of the Presidency Group on Cyber Issues.

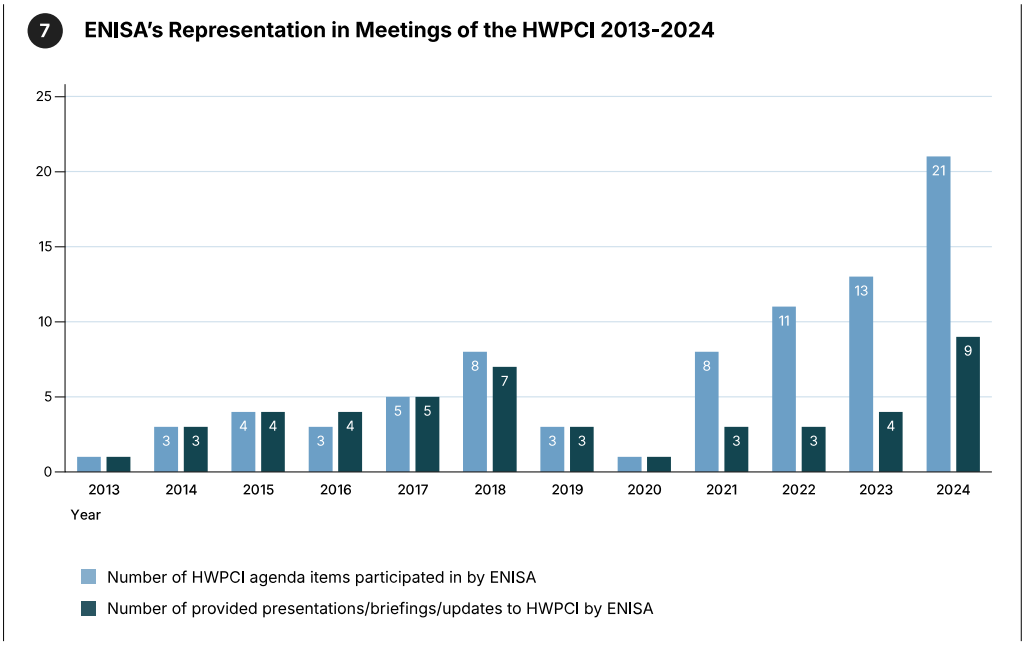

Figure 7: ENISA representation in HWPCI meetings 2013–2024[139]

While representatives of ENISA were often present in the discussion of various agenda items due to the fact that they gave presentations or updates in earlier years, the agency has recently been increasingly involved without having an active presentation role, especially in the context of discussions on the Cyber Diplomacy Toolbox, Cyber Diplomacy Toolbox Tabletop Exercises, EU Cyber Crisis Management, or debriefs provided by the European Union Intelligence and Situation Centre (EU INTCEN). ENISA also added an office in Brussels, operational since April 2022.[140]

Observation 4: ENISA could not shy away from the political backlash surrounding the development of certification schemes

A policy paper on ENISA would not be complete without mentioning the policy-related challenges that have arisen around the establishment of European cybersecurity certification schemes. Past developments in this area also showcase that ENISA cannot entirely avoid having to address politically sensitive issues that may arise within the scope of its mandate. As discussions around the European Union Cloud Services Scheme (EUCS) show,[141] political considerations – and the

139 So far in 2025 (as of March 17, 2025), ENISA participated in 3 HWPCI agenda items and provided 6 presentations/briefings/updates to the HWPCI.
140 European Commission (2024): Draft General Budget of the European Union - Working Document Part III.

lack of a built-in mechanism to deal with divergent Member State views of a (foreign and security) policy nature – have occasionally constrained both the efficiency and the effectiveness of ENISA's work and resulted in frustration among various actors. To diminish the risk of 'deadlocking' ENISA's work on cybersecurity certification schemes, Danish authorities, for instance, highlighted the "need for a mechanism to shift discussion on political matters from ENISA and technical sub groups to a political forum, such as the Council HWPCI" in their publicized response to the European Commission's ENISA evaluation in an effort to separate more political from technical considerations.[142] In his/her reply to the ENISA evaluation, an anonymous member of ENISA's Advisory Group identified the resulting challenge for the agency quite well: "the core of the question is whether the Cybersecurity Act certification system should be used to drive a technical process or should it also pursue more political objectives."[143]

Implications

For ENISA, all these developments raise questions about the agency's ability to remain completely detached from policy issues or political frameworks. In navigating the increasingly complex policy and regulatory landscape it inevitably finds itself in, ENISA must progressively balance its technical mandate with the political realities shaping its work.[144]

Challenge 5: ENISA is taking on a more prominent role at the international level

The CSA not only entrusts ENISA with an inward-looking mandate but also tasks it with "contribut[ing] to the Union's efforts to cooperate with third countries and

141 For further information on the controversies surrounding the EUCS, see, for example, John Salmon, Louise Crawford, Lavan Thasarathakumar, Daniel Lee, Alex Nicol, and Joyce Hoi Wun Leung (2024): EUCS: controversial sovereignty issues continue to drive debate for cloud services, Hogan Lovells, Luca Bertuzzi (2024): LinkedIn Post I, Luca Bertuzzi (2024): LinkedIn Post II, or American Chamber of Commerce to the European Union (2023): Our position: Cybersecurity Certification Scheme for Cloud Services (EUCS).

142 Specifically, the Danish authorities argued that "a political forum can consider political aspects without overshadowing technical certification, ensuring balance and effectiveness" and "separating technical and political considerations fosters transparency, accountability and trust in the certification process," Danish Ministry of Digital Government and Gender Equality & Danish Ministry of Defence (2023): Response to evaluation of ENISA by European Commission. They also appealed for keeping ENISA's involvement technical by noting the following: "ENISA's certification work hinges on technical precision. Political involvement risks compromising objectivity and digital security by introducing biases" and "politicizing ENISA's work may cause decision delays and gridlock, hampering scheme development and threat response." In a similar vein, also industry representatives called for political discussions to "happen before delegating any certification work to ENISA," Information Technology Industry Council (2023): ITI Response to the Consultation on the European Union Agency for Cybersecurity and EU cybersecurity certification framework.

143 Anonymous ENISA Advisory Group Member (2023): Response to evaluation of ENISA by European Commission.

144 This challenge is not unique to ENISA, as it reflects broader debates faced by national agencies like Germany's Federal Office for Information Security (BSI) alike, where controversies such as the Kaspersky product warning have highlighted the difficulty for cybersecurity agencies to balance technical expertise with (geo)political considerations, see, for example, Sven Herpig (2022): Hat das BSI seine politische Unschuld verloren?, Tagesspiegel and Sven Herpig and Manuel Atug (2022), Kaspersky-Produktwarnung: Reine Symbolpolitik?, Tagesspiegel.

international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity" (Art. 12 CSA).[145] As examples to that end, the Act enumerates ENISA participation in international exercises in an observational capacity as well as its support for the European Commission through the provision of advice and expertise, for instance, in the area of mutual recognition of cybersecurity certificates, as well as assuming the role as a facilitator for best practice exchange (Art. 12 CSA).

The CSA also provides for the possibility of "participation of third countries that have concluded agreements with the Union to that effect" (Art. 42(2)).[146] Since 2005, the European Free Trade Association countries Iceland, Liechtenstein, and Norway have participated in ENISA and assume observer roles in the agency's Management Board.[147] The CSA also grants ENISA the opportunity to "cooperate with the competent authorities of third countries or with international organisations or both," with the disclaimer that this cooperation shall be carried out "to the extent necessary in order to achieve the objectives set out in this Regulation" (Art. 42(1)).[148] Any such working arrangement must be previously approved by the European Commission and cannot result in any legal obligations on the part of either the Union or the Member States (Art. 42(1)). Pursuant to a respective provision in the CSA (Art. 42(3)), ENISA developed an international strategy "concerning matters for which ENISA is competent" in November 2021. The strategy outlines ten principles guiding ENISA's international approach, including, for example, provisions on focus, resources, and coordination with/approval by other relevant entities and specifies a portfolio of three international approaches (limited, assisting, and outreach) that ENISA can employ.[149]

In recent years, ENISA has assumed a more prominent role at the international level, evidenced, for example, by the conclusion of working arrangements with Ukrainian[150] and American cybersecurity agencies[151] in June and December 2023

145 Provisions on the international activities of ENISA were also contained in the agency's earlier mandates (Art. 3(1), point (f) Regulation 526/2013 and Art. 3, point (j) Regulation 460/2004).

146 Chamon would label this form of international involvement as "inward external relations" (Merijn Chamon (2019): A constitutional twilight zone: EU decentralized agencies' external relations, Common Market Law Review 56(6)).

147 European Free Trade Association (2018): EEA EFTA Comment on the EU Cybersecurity Agency (ENISA) and the Cybersecurity Act and ENISA (2025): List of ENISA Management Board Representatives and Alternates.

148 Chamon would label this form of international involvement as "outward external relations" (Merijn Chamon (2019): A constitutional twilight zone: EU decentralized agencies' external relations, Common Market Law Review 56(6)). ENISA's international strategy specifies that the agency "will seek endorsement of the Executive Board prior to developing cooperation frameworks or agreements with international organisations and third countries," it must seek approval of its Management Board for cases in which "such agreements place financial or legal obligations on the Agency," ENISA (2021): International Strategy of the EU Agency for Cybersecurity.

149 ENISA (2021): International Strategy of the EU Agency for Cybersecurity.

150 European Commission (2023): Commission Decision approving the Working Arrangement between the European Union Agency for Cybersecurity (ENISA) and the National Cybersecurity Coordination Center of Ukraine (NCCC) and the Administration of the State Service of Special Communication and Information Protection of Ukraine (the Administration of SSSCIP) in the area of cybersecurity, C(2023)4016.

151 European Commission (2023): Commission Decision approving a working arrangement between the European Union Agency for Cybersecurity (ENISA) and the United States Cybersecurity and Infrastructure Security Agency (CISA) in the area of

respectively. A further working arrangement with the NATO Communications and Information Agency (NCIA) is expected to be finalized in due course.[152] A look at the relevant provisions of ENISA's annual activity reports between 2017 and 2023 also underscores the tendency of international expansion of the agency's activities (Table 5):

Year	Activity
2017	• Adoption of "guidelines on international relations" by Management Board
2018	NA
2019	• "ENISA strengthened contacts at an international level in line with the relevant provisions of the new CSA"
2020	• "Some activities were carried out to strengthen[...] contacts at an international level, in particular with the US partners to exchange on lessons learned in response to the pandemic"

2021	• February: Set up of "ENISA task force for international cooperation" "tasked with drafting the ENISA international strategy"
	• November: Adoption of international strategy by Management Board
	• Receipt of "several requests for international cooperation and accommodat[ion of] a number of them"
	Examples:
	  • Provision of "assistance in the context of some cyber dialogues with non-EU countries"
	  • Contributions "to international events organised by the Council of Europe, such as the 2021 Octopus Conference"

2022	Non-exhaustive examples: • Establishment of "agency-wide process [...] to enable international cooperation in accordance with the agency's international strategy policy" • Management of "five outreach engagements and three assisting engagements, and evaluat[ation of] 86 requests for limited engagements" • Establishment of "points of contact and processes to liaise with key EU stakeholders such as EEAS, DG Connect and DG Neighbourhood and Enlargement Negotiations" • Enhancement of "efforts to support the EU action in response to the Russian war of aggression against Ukraine, in particular by moving forward a cooperation agreement with selected Ukrainian entities" • Internal support "with international relations meetings (with Australia, Mauritius, Moldova, Montenegro, Singapore, NATO and the Association of Southeast Asian Nations)" • Establishment of process "for concluding cooperation agreements with international partners" • Participation in EU-Ukraine and EU-USA Cyber Dialogue • Information from 2021 Report: Adoption of an "international strategy

cybersecurity, C(2023)8553.

152 ENISA (2024): ENISA Consolidated Annual Activity Report 2023.

	implementation guidelines" and a "roadmap for the Agency's international partnerships" (both not public to the best of the author's knowledge)
2023	• Conclusion of "working arrangements with the United States and Ukraine" advanced efforts underway for concluding a working arrangement with the NATO Communications and Information Agency (NCIA) • Establishment of "regional strategy to scale international cooperation services for the Western Balkans" • Participation in EU-UK, EU-Japan, and EU-USA Cyber Dialogue, EU–NATO High-Level Staff Talks on Cyber Security and Defence, and the Western Balkan Digital Summit • Management of "141 requests [102 in 2022]: 11 for outreach engagements, 20 for assisting engagements and 110 for limited engagements"

Table 5: Overview of ENISA's international activities 2017–2023 based on the agency's annual activity reports

As a result, and as ENISA itself noted, the expectations of international partners have increased. In this respect, the agency stated in its international strategy (emphasis by the author):

"ENISA is also often approached by third countries directly with **high expectations of mutual collaboration**, and is confronted each time on how best to react. Such welcomed developments **call for a more strategic approach to the international dimension of ENISA's work** in order to guide the engagement of the Agency with third country partners, as well [as] to direct Agency's response to third country partners seeking cooperation with ENISA."[153]

Combined with the observation made in Section 4.2, these developments significantly expand the number of actors likely having expectations towards ENISA by adding international partners as a fifth target audience (see Figure 8):

153 ENISA (2021): International Strategy of the EU Agency for Cybersecurity.

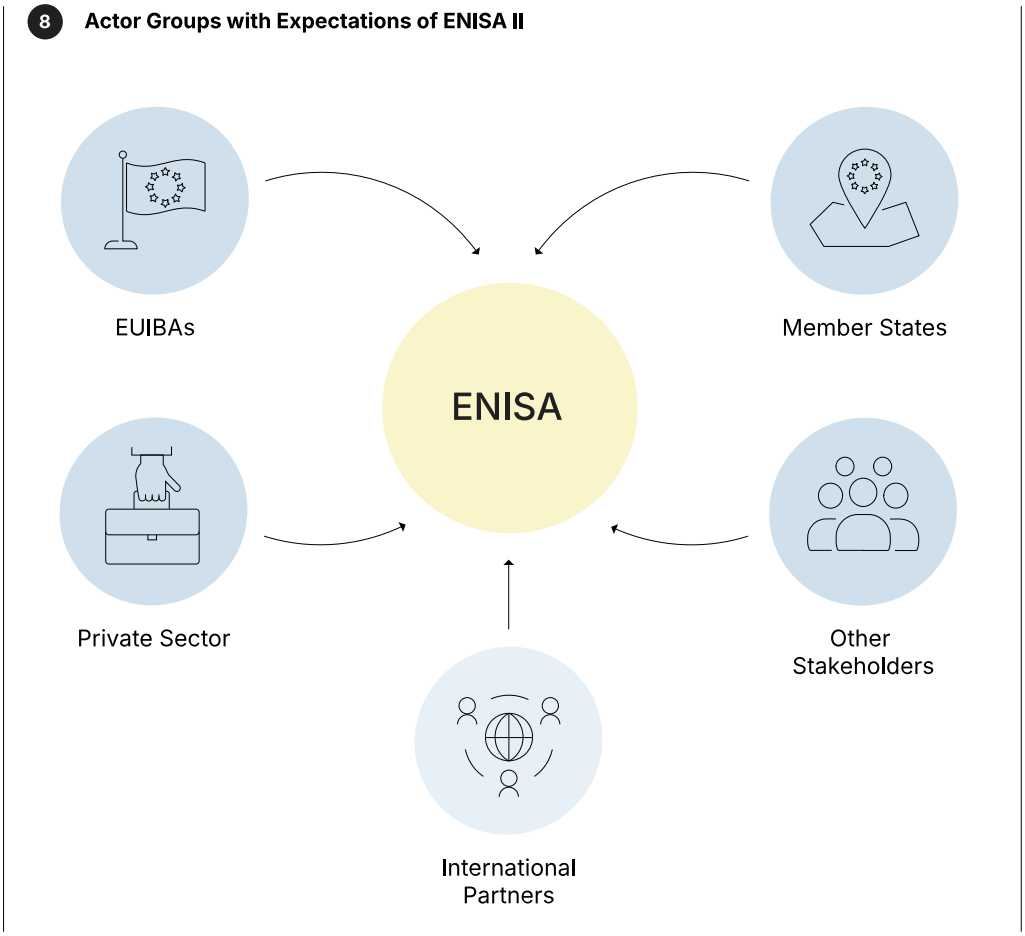

Figure 8: Actor groups with expectations for ENISA II

For instance, a concrete example of these increased expectations for ENISA beyond EU or Member State entities is the interest expressed by stakeholders in having the six Western Balkan economies participate in ENISA (for example, on the basis of Art. 42 CSA).[154] The exact scope of such an involvement would need to be specified in dedicated working arrangements. Judging by ENISA's arrangements with Ukrainian and U.S. authorities, these may center around cyber awareness, capacity-building, or the exchange of best practices.

The Council's conclusions on ENISA also take note of the agency's increased international activities. In this context, EU Member States emphasized that the agency should concentrate its global efforts on key alliances, including the Organization for Security and Co-operation in Europe and NATO, as well as with prospective EU Member States. On a more critical note, the Council also underlined

154 Kosovar Centre for Security Studies (2024): Integration of the Six Countries of the Western Balkans (WB6) in the European Union Agency for Cybersecurity.

"the necessity of clarifying, in accordance with relevant procedures, ENISA's international involvement, ensuring in particular that its Management Board is duly and timely informed of the related activities."[155]

Implications

ENISA's growing international activities may contribute to a blurring of lines of responsibility for the EU's external engagement on cybersecurity and IT security policy at both the EU and Member State levels. ENISA's enhanced international profile also results in a greater need for coordination with key EU players, particularly the European External Action Service (EEAS), as well as the international relations teams within national cybersecurity agencies. This coordination is crucial to ensure coherence and synergies are leveraged where possible. Looking ahead, an important question will hence be whether ENISA's international efforts are "proportionate to the agency's core task"[156] of "ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience, and trust within the Union" (Art. 1(1) CSA). Given the agency's resource constraints, it will also be increasingly relevant for policymakers to determine whether – and if so, how – ENISA should prioritize these international tasks and how many resources should be allocated to that purpose.

Challenge 6: ENISA's workforce needs exceed its allocated budget

Since 2014, ENISA has generally seen an increase in funding and staff, with only a few exceptions in 2018 and 2024 (for a full overview, see Annex III, Section 6.3). Rises were especially granted after the entry into force of the CSA in 2019. However, since the 2024 budget, there has been a gap between ENISA's requests and the resources ultimately allocated to the agency.

For example:

- For the 2025 budget, ENISA requested six additional full-time equivalents (FTEs) and about three million euros more for staff and operational costs.[157] The European

155 Council of the EU (2024): Council conclusions on ENISA, 16527/24.
156 Merijn Chamon (2019): A constitutional twilight zone: EU decentralized agencies' external relations, Common Market Law Review 56(6).
157 For information on what posts are covered by each title, see p. 169 f. European Commission (2024): Draft General Budget of the European Union - Working Document Part III. ENISA emphasized that the additional financial resources for operational expenditure would not "consider[...] the operational budgetary resources which would be necessary to maintain or expand ENISA's ex-ante and ex-post services to Member States under Article 6 and 7 of the CSA, and without the additional costs which it would entail to ensure corporate and administrative support."

Commission granted two additional posts (one temporary and one seconded national expert (SNE)) as stipulated in the CRA's legislative financial statement and did not increase the budget as requested.

- In 2024, ENISA asked for an eight million euro budget increase and 17.5 more FTEs to meet its growing responsibilities,[158] none of which it ultimately received.[159] With a view to carrying out new tasks conferred to ENISA through the CRA and CSOA, ENISA, based on estimates, requested an additional allocation of 8.33 FTEs (on average) per year for the years 2025–2027.[160]

The issue of ENISA's limited human resources dates back to the agency's early years. In 2007, an evaluation of ENISA came to the conclusion that it should employ "at least 100 staff."[161] At the time, ENISA employed 56. During the 2017 evaluation of ENISA, "38 of 54 respondents to the online public consultation expressed the view that the size of the agency was inadequate."[162] At the time of the latter evaluation, ENISA employed 84 persons. This number had risen to 113 by 2023 (for more details on ENISA's budgetary and human resources over the years see Section 3.7).[163] The agency surpassed the number of 100 employees for the first time in 2021.[164]

ENISA has responded to these – in its view – unfavorable resource-related developments by becoming increasingly vocal, openly criticizing the significant gap between its requested and allocated resources. It also warned that it is nearing the limits of its operational capacity as a result. To make its case for increased budgetary and human resources, ENISA has put forward a number of arguments over the years:

1. First and foremost, ENISA argues that its resources do not reflect the increasing tasks assigned by **new legislation and stakeholder expectations**.[165] In 2023, ENISA's

158 European Commission (2023): Draft General Budget of the European Union - Working Document Part III.

159 Interestingly, that year, the position of the European Parliament was roughly 1.5 million euros higher than that of the Council, Council of the EU General Secretariat (2023): Joint text on the general budget of the European Union for the financial year 2024: Amendments by budget line - Consolidated document (integration of agreed amendments on DB or Council's position): Section III - Commission.

160 European Commission (2024): Draft General Budget of the European Union - Working Document Part III, CRA: 9 FTEs (3 in 2025, 4 in 2026, 2 in 2027) and CSOA: 16 FTEs (3 in 2025, 5 in 2026, 8 in 2027). Previously, in the context of the NIS 2 Directive, ENISA did receive limited additional resources. To undertake its tasks pursuant to the NIS 2 Directive, ENISA received five new posts and an additional monetary contribution of roughly 600 thousand euros, which ENISA also deemed insufficient (European Commission (2023): Draft General Budget Of The European Union - Working Document Part III). In this respect, however, ENISA claimed that these additional resources would "fall far short to the initial needs which the Agency put forward during the consultations with the Commission (10-12 posts) [...] nor were the final additional resources qualitatively fit for purpose."

161 European Commission (2007): Communication from the Commission to the European Parliament and the Council on the evaluation of the European Network and Information Security Agency (ENISA).

162 European Commission (2017): Commission Staff Working Document on the evaluation of the European Union Agency for Network and Information Security (ENISA) Accompanying the document Proposal for a regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

163 European Court of Auditors (2024): Annual report on EU agencies for the financial year 2023.

164 In that year, the agency employed 106 persons. For comparison, the agency employed 87 persons in the year prior.

165 In 2022, during its annual workforce review, ENISA estimated needs amounting to "additional 41.5 FTEs in order to address all external as well as internal expectations," emphasizing that the amount put forward "did not cover fully the needs arising from CRA nor CSOA," European Commission (2024): Draft General Budget of the European Union - Working Document Part III). The

Management Board raised its concerns in a letter to then Commissioner Thierry Breton in order "to ensure adequate resources for the Agency to be able to undertake any new tasks."[166] ENISA underscored its commitment to "continuous improvement of its administrative and operational efficiency," but also claimed that it would have "almost exhausted all possible internal and external actions that it can take to resolve the insufficient allocated resources."[167]

2. In addition, ENISA complained that, as a side effect, the de-/re-prioritization resulting from limited resources would have resulted in **internal reshufflings** and rededication of both resources and personnel due to ad hoc adjustments, with the Cybersecurity Support Action representing one example.[168]

3. Another major concern of the agency is the "rapidly **deteriorating cybersecurity threat landscape**," worsened by the war in Ukraine, which ENISA argues was not foreseen in the EU's 2021-2027 MFF.[169] ENISA claims that even with the additional funds dedicated to it via the Cybersecurity Support Action following the Nevers Call,[170] this financial contribution would not be enough for it to carry out the tasks assigned to it and meet the interests of various stakeholders.[171] In this context, the Management Board has asked for "increased human resources that also include an **operational reserve component** to be able to manage heightened cybersecurity challenges during times of escalation" in order to be prepared to avoid the need for reactive ad hoc readjustment.[172]

4. Lastly, proponents of increased resources for ENISA emphasize the extensive consequences resulting from its constrained resources both in terms of its ability to act and the implications for the attainment of its objectives. These consequences are specifically described as being "**detriment[al] to the agency's ability to achieve a high common level of cybersecurity** across the Union."[173]

---

agency also pointed to the high costs for Member States to comply with the NIS 2 Directive. While acknowledging that it "does not fulfil the regulatory duties in the same way," ENISA made the argument that "most Member States have responded to NIS2 by significantly increasing the staff numbers of their national cybersecurity agencies," European Commission (2023): Draft General Budget of the European Union - Working Document Part III.

166 ENISA (2024): Decision No MB/2024/08 of the ENISA Management Board on analyses and assessment of the Annual Activity Report 2023.

167 European Commission (2023): Draft General Budget of the European Union - Working Document Part III.

168 In order to implement the Cybersecurity Support Action, ENISA "had to redirect internal resources (approx. 10 FTEs) from other activities in order to properly implement this support action for Member States" as it was not granted any additional posts (European Commission (2023): Draft General Budget of the European Union - Working Document Part III). The redirected internal resources amount to roughly 16 percent of ENISA's available human resources in 2022. In this respect, ENISA's Management Board "acknowledge[d] the strain on human capital due to insufficient operational reserves available to the Agency to manage times of escalation," ENISA (2023): Decision No MB/2023/07 of the Management Board of the European Union Agency for Cybersecurity (ENISA) on analyses and assessment of the Annual Activity Report 2022.

169 European Commission (2023): Draft General Budget of the European Union - Working Document Part III.

170 Council of the EU (2022): Nevers Call to Reinforce the EU's Cybersecurity Capabilities.

171 European Commission (2023): Draft General Budget of the European Union - Working Document Part III.

172 ENISA (2023): Decision No MB/2023/07 of the Management Board of the European Union Agency for Cybersecurity (ENISA) on analyses and assessment of the Annual Activity Report 2022.

173 ENISA (2024): Decision No MB/2024/08 of the ENISA Management Board of 6 June 2024 on analyses and assessment of the Annual Activity Report 2023. For example, in its justification for the additional resources for 2025, ENISA underscored the following: "By the end of 2024, if the already announced legislative and political expectations towards the Agency will materialise ENISA's budgetary and human resource means shall be drawn to their absolute limits. Unless the FTE needs stemming from new tasks are addressed, the Agency will need to severely limit and deprioritise its existing operational activities in 2025 and 2026 within the programming period of 2025-2027, in order to reallocate FTEs to new emerging tasks. This will in turn limit ENISA's ability to deliver its overall mandate and objectives in their entirety," European Commission (2024): Draft General Budget of the European Union - Working Document Part III. On the same occasion one year earlier, ENISA argued that "with the long-term outlook of the Union threat landscape remaining gloomy, the Agency cannot, under its current normal budgetary and human resource limits, maintain even the minimum level of support it has been able to muster in 2022, without jeopardising its other priorities, like increasing assistance to the Union and Member States to support the transposition of NIS2 or support the actual deployment of new certification schemes," European Commission (2023): Draft General Budget of the European Union - Working Document Part III.

With the Council conclusions on ENISA, Member States again made the case for equipping ENISA with "adequate resources – human, financial and technical – in order to fully enable the Agency to execute all the tasks under its competence," and therefore called on the European Commission "to prioritise actions and assign priority to tasks related to supporting Member States in enhancing their cyber resilience, their operational cooperation and the development and implementation of Union Law when preparing the draft general budget of the Union."[174]

Implications

Faced with these resource constraints, ENISA finds itself in a situation where it has to square the circle. On the one hand, to make a compelling case for increased resources across the Union, decision-makers would benefit from firsthand experiences of ENISA's added value. On the other hand, ENISA lacks the resources necessary for effective outreach and communication reaching decision-makers in Member States, which could influence political support. This creates a dilemma: ENISA needs greater visibility – particularly in national capitals – to justify its funding needs, yet it struggles to achieve this visibility without the resources it seeks.

In its 2023 Coordinated Annual Activity Report, the agency acknowledged "overlaps, gaps, and inconsistencies in existing policies,"[175] underscoring that the agency's limited resources can not only hinder its ability to act but might also prevent it from effectively monitoring, identifying, and resolving regulatory discrepancies. This challenge is particularly fundamental given the recent expansion of the EU's cybersecurity policy ecosystem, where a lack of oversight and management of interlinkages across policies risks weakening the Union's overall objective of enhancing cybersecurity throughout Europe through the establishment and enforcement of a legally sound and consistent framework. Limited resources may also negatively affect the agency's working environment. This risk is evidenced in ENISA's 2023 Annual Activity Report, which noted that "staff satisfaction was below the target value, driven mainly by time management and stress levels."[176]

174 Council of the EU (2024): Council conclusions on ENISA, 16527/24.

175 ENISA (2024): ENISA Consolidated Annual Activity Report 2023.

176 ENISA (2024): ENISA Consolidated Annual Activity Report 2023. In earlier years (2021), the activity report also mentioned that "nearly one quarter of ENISA staff find that they have limited opportunities to grow within the Agency, and are not satisfied with their work," ENISA (2022): Consolidated Annual Activity Report 2021. During an extraordinary ENISA Management Board meeting, ENISA's Executive Director also alluded to "rivalry and lack of trust," "misfit between talent and function, function and aims," as well as "talent management" as being among a few of the agency's problem areas, ENISA (2020): ENISA Management Board Extraordinary Meeting held on 3 February 2020 in Athens, Greece.

Recommendations

Disclaimer:

The recommendations included in this section were developed before ENISA published its 2025–2027 Single Programming Document (SPD) in February 2025. This document is noteworthy, as it may indicate a shift in the agency's approach hinting at a shared recognition among both Member States and the European Commission of the need to reform ENISA. While the specifics and rationales of why certain decisions were made were not communicated, apart from a general objective to "more effectively manage the[agency's] activities and improve [its] capacity to deliver more efficiently,"[177] the SPD specifies that ENISA deprioritized certain activities, readjusted its strategic objectives, and reorganized its internal structure.[178] It appears from these changes that ENISA should intend to focus more comprehensively on activities related to operational cooperation and policy implementation.[179] Whether these steps will yield the desired outcomes – some of which are in line with the recommendations made below – is yet to be determined. If the intended results materialize, they can represent a positive move toward addressing some of the agency's long-standing challenges outlined earlier.

As Chapter 4 has shown, ENISA has undergone significant shifts in recent years. In theory, ENISA is well-positioned to assist various stakeholders. However, in practice, the agency often falls short of meeting the expectations placed upon it. As the Union positions itself as a global driver and leader in setting norms and standards on cybersecurity, its dedicated agency for cybersecurity matters faces challenges due to resource-induced capacity gaps, mandate unclarity, and operational efficiency, which may impact internal policy cohesion and the EU's external leadership potential. The challenges outlined in Chapter 4 highlight the need for ENISA, and particularly the political levels involved, to more clearly define

177 .

178 It should be noted that the SPD does not explicitly lay out which changes were made. When comparing the work program, internal structure, and strategic objectives with their predecessor documents, the following specific changes appear to have been taken by the Management Board: As part of the agency's 2025 work program, the Management Board has deprioritized earlier activities related to emerging cybersecurity challenges, outreach and education, and research and innovation needs. However, some outputs from these areas have been integrated into other activities, such as the development and maintenance of the EU cybersecurity index now falling under policy monitoring and development activity, ENISA's international strategy and outreach moving to operational cooperation, and the EU cybersecurity skills framework becoming part of the agency's capacity-building efforts. These changes are also evident in the agency's internal restructuring, where the exercises and training sector was discontinued, while cybersecurity and resilience of critical sectors was elevated to a full unit. The operational cooperation unit was expanded with a new sector dedicated to crisis response and stakeholder support. Additionally, two new units were created: the Operational and Situational Awareness (OSA) unit, which includes a threat analysis service and an incidents and vulnerabilities service, as well as an operational and support unit for implementing the Cybersecurity Support Action. The market, certification, and standardization unit was split into two units, with one focusing solely on certification and the other on market, technology, and product security. Meanwhile, the policy development and implementation unit adjusted its scope to cover policy monitoring and analysis. While ENISA's strategic objectives remain largely unchanged, two adjustments highlight an increased focus on implementation, shifting from integrating cybersecurity into EU policies to actively supporting their execution, and elevating effective cooperation to a broader goal of enhancing Union-wide preparedness and response.

179 These measures can also be seen as a follow up to the Council's December 2024 conclusions on the future of ENISA, in which Member States, inter alia, encouraged the European Commission "to consider streamlining ENISA's role in respect of tasks that are not at the core of its mission," .

the agency's role, better articulate its priorities, and effectively target key audiences to manage expectations.

Recommendation 1: Clarifying ENISA's role

Since its establishment, the scope of tasks assigned to ENISA as well as the importance of cybersecurity at the EU level accelerated significantly. In recent years, for example, ENISA has taken on a larger role in coordinating Member States' activities at the operational level, developing EU policies, and raising its international profile. At the same time, the boundaries between ENISA's competences and those of other EU and national entities remain blurred, as does the agency's primary objective of contributing to the "functioning of the internal market" (Art. 114 TFEU).

Additionally, divergences in preferences regarding ENISA's role exist among Member States. For instance, some Member States may want ENISA to take on a larger role in incident response due to their own limited resources, while others prefer that ENISA does not communicate directly with, for example, domestic companies affected by a particular incident. At the same time, the agency faces the challenge of balancing its technical mandate with the inevitable political components surrounding cybersecurity, playing out especially at the EU level. Meanwhile, the European Commission is bringing more power in terms of cybersecurity policy to the EU level by extending its policy and regulatory efforts – and ultimately also its competences – in this domain, yet it has not expanded ENISA's role accordingly. This underscores the need for a sharper delineation of ENISA's activities and a clearer articulation of the stakes the agency holds in EU cybersecurity (policy).

To optimize ENISA's impact, particularly in the context of its limited resources, it is crucial for policymakers to clarify the agency's role and specify where ENISA, as an EU agency, adds the most value in enhancing the Union's cybersecurity. In this respect, pinpointing tasks and responsibilities that ENISA could best handle in collaboration with, or in support of, other entities that may already be carrying out part of the work could help optimize ENISA's resource capacity.

Recommendation 2: Refining prioritization of ENISA activities

An unclear role and insufficiently delineated target audiences hinder ENISA's ability to focus and specialize. ENISA's horizontal mandate and current setup require significant resources for coordinating and maintaining close relationships with

actors across EUIBAs, Member States, industry, other stakeholders, and international partners – each with interconnected but varied objectives. At the same time, ENISA's limited resources necessitate sharper prioritization, with a focus on clearly defined actions that align with its strategic objectives. For instance, in its 2023 Annual Activity Report, the agency noted that "activity 1 [providing assistance on policy development], jointly with activity 2 [supporting implementation of Union policy and law[180]], topped the ENISA Management Board's list of priorities."[181] If this is the shared assessment of Member States and the European Commission, these priorities – along with the full ranking – should be communicated widely and explicitly rather than be left to implicit inference.[182] An enhanced prioritization would permit ENISA to develop specialized expertise for priority areas in a sustainable manner while at the same time fostering trusted relationships with primary recipients of its activities.

Recommendation 3: Manage expectations of ENISA's target audiences

As Figure 8 underscores, a wide variety of actors have high expectations for ENISA. However, neither ENISA nor the political leadership defining its mandate appear to have effectively managed these expectations, as evidenced by the publicized responses to the European Commission's evaluation of ENISA.[183] To address this, both ENISA and policymakers should clearly communicate – particularly with the private sector, other stakeholders, and international partners – what level of support they can realistically expect from ENISA given the agency's resource constraints. To ensure transparency and clarity, it is essential that relevant actors understand the criteria by which ENISA prioritizes its activities and stakeholder engagement. While this information does not always need to be publicly available, it should be shared with key stakeholders, especially considering the varying levels of maturity and capability among those seeking ENISA's assistance. Additionally, if ENISA lacks the resources to engage further, communicating this proactively would help mitigate potential misunderstandings and manage expectations based on a realistic assessment of the agency's capacity.

As a starting point, ENISA could build upon its 2022 stakeholder strategy, which is

180 There is a need for such activities since ENISA said it supported 12 Member States in the implementation of the NIS 2 Directive through "advice on the directive's transposition to national legislation and organised risk management trainings for national authorities to help build up knowledge and expertise," ENISA (2024): ENISA Consolidated Annual Activity Report 2023.

181 ENISA (2024): ENISA Consolidated Annual Activity Report 2023.

182 The need to increasingly shift from implicit inference to explicit communication is also underscored by how ENISA has most recently communicated changes to its internal structure and the de-prioritization of activities. See further the disclaimer at the beginning of this chapter and footnote 180.

183 European Commission (2023): European Union Agency for Cybersecurity and EU cybersecurity certification framework – evaluation.

not publicly available, by enhancing transparency around stakeholder engagement. Expanding on recent good communication practices – such as listing stakeholders and engagement levels for each agency activity in its work program[184] and specifying topics and content for intended target audiences, as seen with ENISA's new website[185] – can improve clarity and make the strategy more visible as a reference point. Effective expectation management would also benefit significantly from a clearer definition of ENISA's role (Recommendation 1) and a sharper prioritization of the agency's activities (Recommendation 2).

Making ENISA fit for purpose is a question of political will

Meeting the EU's formulated cybersecurity-related objectives requires a strong institutional backbone. Addressing the challenges outlined in this paper is therefore essential to preserving the EU's regulatory and policy entrepreneurship on cybersecurity matters. If ENISA's mandate is to be revised during this legislative cycle, policymakers should act on these recommendations. But how can this be achieved?

A first step in implementing these recommendations would be a more proactive and transparent communication strategy by ENISA, the European Commission, and Member States. This should include clear engagement with EU and national entities, organizations bound by EU cybersecurity legislation, and the public.[186] Enhanced transparency and targeted outreach would help stakeholders better understand ENISA's actions and priorities – an issue Member States have also previously identified as requiring improvement.[187]

184 As part of this strategy, since the agency's 2023 work program, ENISA has been listing stakeholders and levels of engagement for each of its activities. In this context, the work program distinguishes between "partner" or "involve/engage" stakeholders. ENISA defines them as follows: "Stakeholders classified as 'partner' refers to stakeholders with high influence and high interest, usually business owners and others with significant decision-making authority. They are typically easy to identify and to engage with actively. Stakeholders classified as 'involve/engage' have high influence but low interest. These are typically stakeholders with a significant decision-making authority but lacking the availability or the interest to be actively engaged" (ENISA (2025): ENISA Single Programming Document 2025-2027). In a more limited manner, in 2021 and 2022, the agency listed target groups and beneficiaries in this context.

185 The three groups ENISA refers to in this respect are: (1) national and EU authorities, (2) the private sector, and (3) citizens.

186 Vis-à-vis the public, in the area of knowledge and information, the CSA entrusts ENISA to "pool, organise and make available to the public information on cybersecurity provided by the Union institutions, bodies, offices and agencies and information on cybersecurity provided on a voluntary basis by Member States and private and public stakeholders" by means of "a dedicated portal" (Art. 9, point (d)).

187 For example, Czechia complained about a "lack of transparency when decisions are being made," advocating for ENISA in the future to "communicate its plans and steps with the Member States in advance and as openly as possible, especially if the Member States are to be actively engaged in such efforts" within their response to the Commission's evaluation on ENISA. NUKIB, Czechia's central administrative body for cybersecurity, also highlighted "space for improvement regarding the transparency of ENISAs activities, which currently seem to work on an ad hoc basis without proper planning and without ex post review of whether plans have been fully met" and "a lack of transparency in communication from ENISAs side regarding the proposed certification schemes" (National Cyber and Information Security Agency of the Czech Republic (2023): Response to evaluation of ENISA by European Commission). Communication was also a concern raised by the Danish authorities, which they addressed specifically in the context of "processes for establishing certifications." The Danish authorities also "request[ed] a larger degree of transparency in the proceedings of the ad hoc working groups" (Danish Ministry of Digital Government and Gender Equality & Danish Ministry of Defence (2023): Response to evaluation of ENISA by European Commission).

Ultimately, however, ENISA's future depends on political will. The agency cannot drive meaningful change on its own, as these issues lie beyond its direct scope of influence and decision-making authority (for an overview of ENISA's governance structures see Section 3.4, Section 3.5, Section 3.6, and Annex I, Section 6.1). Progress will require strong backing from both Member States and the European Commission, which together form ENISA's Management Board. One way to structure this support could be by integrating an ENISA-specific work package into the mid-term program for Council presidencies, developed by the 'trio groups'.[188] Securing additional support from policymakers in the European Parliament could reinforce this effort. The recent Council conclusions on ENISA[189] as well as the 'Warsaw Call' declaration by EU ministers responsible for cybersecurity,[190] which emphasized the "need for a strengthened, clearly defined, and focused ENISA [...] mandate," provide a strong foundation for mobilizing further support and reinforcing Member State commitments.

To implement the recommendations outlined in this Chapter, policymakers in Member States and EU institutions must decide whether to provide ENISA with the necessary resources, capabilities, and political backing. **Two basic conceptual options emerge in that regard: Either decisionmakers equip ENISA with the financial resources and personnel needed to fully meet its mission and responsibilities or, on the contrary, they decide in favor of redefining ENISA's mandate so that it aligns with existing resources.** The latter would require significantly narrowing ENISA's tasks, limiting its scope of activities – such as focusing solely on policy implementation, capacity-building, and/or certification – and/or restricting the agency's role to provide support exclusively to Member States and EUIBAs,[191] thereby also decreasing the number of actors placing expectations on ENISA.

To facilitate finding consensus on which pathway to take, policy and decision-makers should comprehensively address the following questions when seeking to clarify ENISA's role, refine its priorities, and manage expectations more effectively:

1. Clarifying ENISA's role

- What (complementary) role(s) should ENISA assume? Should ENISA be

188 The trio groups are the rotating trio of Member States holding the Council presidencies.

189 Council of the EU (2024): Council conclusions on ENISA, 16527/24.

190 Polish Presidency of the Council of the European Union (2025): Warsaw Call Declaration adopted at the informal TTE Telecom Council on cybersecurity.

191 Both are alluded to as "key beneficiaries" in ENISA's 2025–2027 Single Programming Document.

predominantly associated with the role of capacity-builder, operational facilitator, policy developer, or something else?

- How is ENISA's role distinct from that of other dedicated cybersecurity actors at the EU level, such as the ECCC, CERT-EU, or the Cyber Situation and Analysis Centre?
- In which areas does ENISA assume the lead at the EU level (if so)?
- How are synergies best leveraged (and duplications avoided) in the interplay between ENISA's activities and those of Member State entities?
- How much of an operational and political actor should ENISA become? What degree of involvement would ultimately be considered as too operational or too political by which actors?
- How independent can/should ENISA be and act in the future?
- What constitutes a proportionate balance between ENISA's international efforts and its activities within the Union?

2. Refining prioritization of ENISA activities

- What is ENISA's core objective, signature task, and flagship activity?
- In which areas does ENISA offer the greatest added value? For example, EU-level strategic guidance, fostering interoperability, supporting cross-border initiatives, or carrying out exercises?
- How can ENISA ensure that existing resources and best practices at the Member State level are better shared and utilized regionally across jurisdictions or comprehensively at the EU level?

3. Managing expectations of ENISA's target audiences

- What actor group(s) represent(s) ENISA's main target audience? For example, should ENISA focus its activities on Member State and EU entities as priority target audiences?
- What specific actors should ENISA focus on within these groups? For example, vis-à-vis EU entities, should ENISA focus on the least mature EUIBAs?
- Which actor at which political level is best positioned to reach specific target audiences outlined in ENISA's mandate, also bearing in mind the principle of subsidiarity?
- What are the most effective ways and channels for ENISA – or the political levels steering its operations – to reach various audiences and communicate what ENISA can and, more importantly, cannot do for them?

Outlook

With the agency's role under review as part of the European Commission's ongoing evaluation mandated by the CSA, 2025 marks a pivotal moment for reassessing ENISA's capacity and clarifying its strategic direction. Looking ahead, two issues stand out:

First, resources will remain a crucial factor. As the number of entities subject to new

obligations grows, ENISA will require innovative solutions for effective implementation – especially given the similar challenges faced by Member States. At the same time, there should be no illusion that more resources are in themselves the silver bullet and solution to ENISA's challenges. They would need to be accompanied by reforms to internal processes to ensure that they are used in the most efficient manner. The negotiation of the next EU MFF post-2027 will be a critical window of opportunity for those advocating for increased resources for ENISA.

Second, in clarifying ENISA's role, policymakers and decision-makers should determine whether the agency should continue to operate within its role as an "internal market agency" or if its mandate should be explicitly elevated to encompass matters beyond the internal and digital single market. With its responsibilities continuing to expand, ENISA is already de facto functioning as more than an exclusively internal market–oriented entity, reflecting its evolving and increasingly complex mandate. How ENISA's operational role will evolve and how it navigates political dynamics in the coming years will shape both its designated role and the expectations placed upon it.

Taking the steps necessary to act on one of the proposed options, rather than maintaining the below-par status quo, is essential for the EU to effectively manage – and more importantly implement – its ever-expanding cybersecurity policy framework.

Annex

ENISA's governance structures

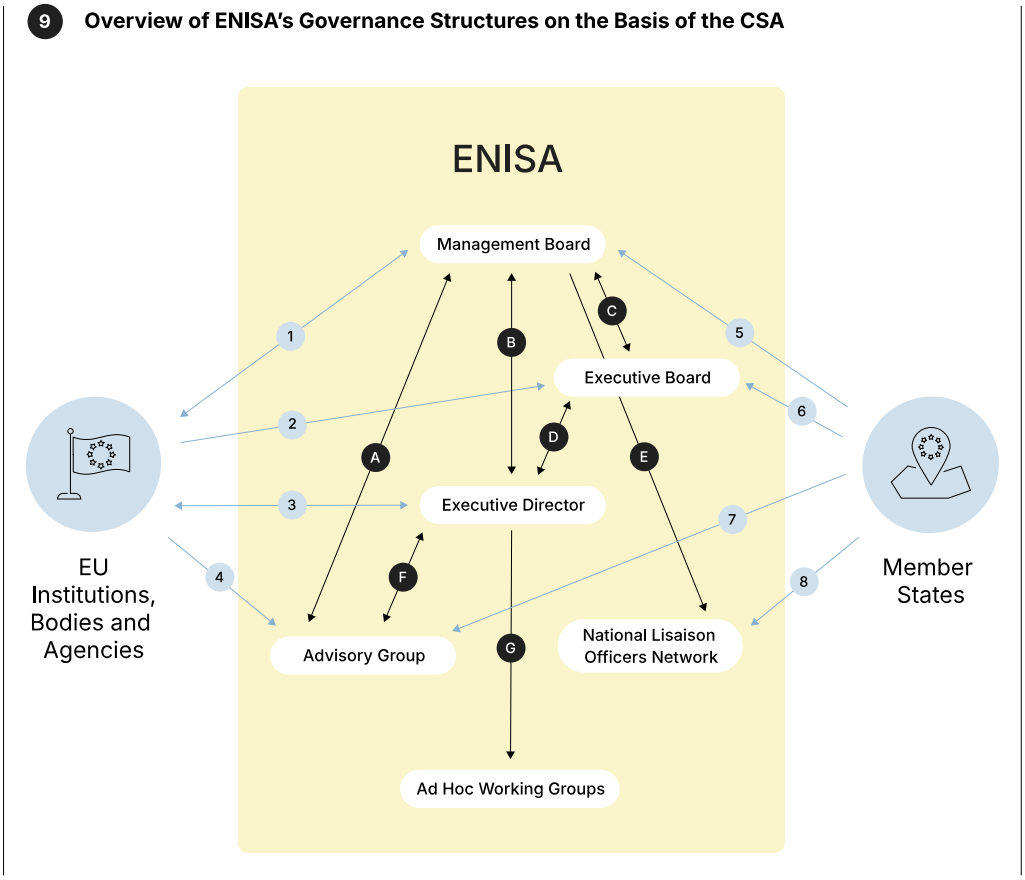

Figure 9: Overview of ENISA's governance structures on the basis of the CSA

Below, you can expand on various sections to explain the connections between the actors. The numbers and letters correspond to those contained in Figure 9 above. All article references in the table below relate to the Cybersecurity Act, Regulation 2019/881.

---

①

Management Board → European Commission

• Upon adoption of ENISA's draft single programming document, "submission to the Commission for an opinion" (Art. 15(1), point (b))

• Adoption of ENISA's single programming document "taking into account the Commission's opinion" (Art. 15(1), point (c))

• Submission of ENISA's "annual report and the assessment thereof by 1 July of the

following year" (Art. 15(1), point (f))

• Submission of single programming document, including a "statement of estimates", "by 31 January of the following year" and "any subsequently updated versions of that document" (Art. 24(3) and Art. 29(3))

• Consultation of European Commission before adoption of the "financial rules applicable to ENISA" (Art. 32)

Management Board → Council

• Submission of ENISA's "annual report and the assessment thereof by 1 July of the following year" (Art. 15(1), point (f))

• Submission of single programming document "by 31 January of the following year" and "any subsequently updated versions of that document" (Art. 24(3))

Management Board → European Parliament

• Submission of ENISA's "annual report and the assessment thereof by 1 July of the following year" (Art. 15(1), point (f))

• Submission of single programming document "by 31 January of the following year" and "any subsequently updated versions of that document" (Art. 24(3))

• Information "about its intention to extend the Executive Director's term of office" (Art. 36(8))

Management Board → Court of Auditors

• Submission of ENISA's "annual report and the assessment thereof by 1 July of the following year" (Art. 15(1), point (f))

European Commission → Management Board

• Representation of European Commission in ENISA Management Board by appointment of two members, each having the right to vote (Art. 14(1))

• The European Commission can request the Management Board to convene an extraordinary meeting (Art. 17(2))

• Preparation of a proposal including a "list of candidates" for the position of ENISA Executive Director (Art. 36(2)) and a proposal on the extension of the ENISA Executive Director's tenure (Art. 36(7)) or his/her removal (Art. 36(10))

• Transmission of "a report on the evaluation of ENISA [Art. 67(1)] together with its conclusions" (Art. 67(4))

---

②

European Commission → Executive Board

• Representation in ENISA Executive Board by at least one member (Art. 19(3))

---

③

Executive Director → European Commission

• Biennial reporting by the Executive Director on progress with respect to an "action plan that follows up on the conclusions of the retrospective evaluations" (Art. 20(3), point (f))

• Annual transmission of the "report on the budgetary and financial management" "by 31 March of year N + 1" (Art. 31(6))

• Submission of a copy of his/her reply to the European Court of Auditor's observations "by 30 September of year N + 1" (Art. 31(10))

• Consultation of European Commission in the "prepar[tion of] a proposal for ENISA's annual work programme" (recital (59))

• Biennial reporting by the Executive Director on the progress with respect to "an action plan that follows up on the conclusions of internal or external audit reports, as well as on investigations by OLAF" (Art. 20(3), point (g))

Executive Director → European Parliament

• Upon invitation, report to the European Parliament "on the performance of his or her duties" (Art. 20(2))

• Annual transmission of the "report on the budgetary and financial management" "by 31 March of year N + 1" (Art. 31(6))

• Upon request by the European Parliament, submission of "any information required for the smooth application of the discharge procedure for the financial year concerned" (Art. 31(11))

• Upon invitation, "within three months before any such extension [extension of the Executive Director's term of office]", provision of "a statement before the relevant committee of the European Parliament and answer Members' questions" (Art. 36(8))

Executive Director → Council

• Upon invitation, report to the Council "on the performance of his or her duties" (Art. 20(2))

• Annual transmission of the "report on the budgetary and financial management" "by 31 March of year N + 1" (Art. 31(6))

Executive Director → Court of Auditors

• Annual transmission of the "report on the budgetary and financial management" "by 31 March of year N + 1" (Art. 31(6))

• Submission of a reply to the European Court of Auditor's observations "by 30 September of year N + 1" (Art. 31(10))

Executive Director → EUIBAs

• Regular exchange of "views and information [...] with Union institutions, bodies, offices and agencies regarding their activities relating to cybersecurity to ensure coherence in the development and the implementation of Union policy" as part of the Executive Director's responsibilities (Art. 20(3), point (m))

European Commission → Executive Director

• "Assessment of the performance of the Executive Director and ENISA's future tasks and challenges" after the end of an Executive Director's term of office (Art. 36(5))

• In the context of ENISA's cooperation with third countries and international organisations, conclusion of "appropriate working arrangements with the Executive Director" in an effort to "ensure that ENISA operates within its mandate and the existing institutional framework" (Art. 42(3))

Parliament → Executive Director

• Provision of "discharge to the Executive Director in respect of the implementation of the budget for the year N" (Art. 31(12))

---

④

European Commission → Advisory Group

• Right to "be present at the meetings of the ENISA Advisory Group and to participate in its work" (Art. 21(4))

---

⑤

Member States → Management Board

• Representation of each Member State in ENISA Management Board by one appointed Member each, each having the right to vote (Art. 14(1))

⑥

Member States → Executive Board

• Appointment of Executive Board members "among the members of the Management Board" (Art. 19(3))

⑦

Member States → Advisory Group

• Right to "be present at the meetings of the ENISA Advisory Group and to participate in its work" (Art. 21(4))

⑧

Member States → NLO Network

• Appointment of one representative to the NLO Network (Art. 23(1))

Ⓐ

Management Board → Advisory Group

• Upon invitation by Management Board Chairperson, participation of ENISA Advisory Group members in Management Board meetings without the right to vote (Art. 17(4))

• Establishment of the ENISA Advisory Group (Art. 21(1))

Advisory Group → Management Board

• Regular information of the Management Board of the ENISA Advisory Group's activities (Art. 21(6))

Ⓑ

Management Board → Executive Director

• Opportunity of "delegat[ing] the power to make non-substantial amendments to the annual work programme to the Executive Director" (Art. 24(6))

• Appointment of Executive Director (Art. 36(2))

• Responsibility for decision of extension of Executive Director's tenure (Art. 36(7)) or on his/her removal (Art. 36(10))

Executive Director → Management Board

• Participation in Management Board meetings without the right to vote (Art. 17(3))

• Accountability of Executive Director towards Management Board (Art. 20(1))

• Responsibility for "implementing the decisions adopted by the Management Board" (Art. 20(3), point (b))

• Submission of ENISA's draft single programming document to Management Board for approval (Art. 20(3), point (c))

• Responsibility for implementing and "reporting to the Management Board" on the single programming document's implementation (Art. 20(3), point (d))

• Presentation of "the consolidated annual report on ENISA's activities, including the implementation of ENISA's annual work programme" to the Management Board for their "assessment and adoption" (Art. 20(3), point (e))

• Preparation of a proposal for the composition of the ENISA Advisory Group (Art. 21(1))

• Preparation of a proposal for the establishment of the National Liaison Officers Network (Art. 23(1))

• Annual transmission of a "draft statement of ENISA's revenue and expenditure for the following year [...] together with a draft establishment plan" (Art. 29(1))

• Submission of an "anti-fraud strategy for ENISA" for Management Board approval (Art. 20(3), point (k))

• Regular reporting by the Executive Director on the progress with respect to "an action plan that follows up on the conclusions of internal or external audit reports, as well as on investigations by OLAF" (Art. 20(3), point (g))

• When setting up ad hoc working groups, provision of advanced notice to Management Board (Art. 20(4))

• Submission of a copy of his/her reply to the European Court of Auditor's observations "by 30 September of year N + 1" (Art. 31(10))

Management Board → Executive Board

• Appointment of Executive Board members "from among the Members of the Management Board" (Art. 19(3))

• Adoption of the Executive Board's rules of procedure (Art. 19(6))

Executive Board → Management Board

• Assistance of Management Board (Art. 19(1))

• "Prepar[ation of] decisions to be adopted by the Management Board" (Art. 19(2), point (a))

• "When necessary because of urgency, the Executive Board may take certain provisional decisions on behalf of the Management Board, in particular on administrative management matters, including the suspension of the delegation of the appointing authority powers and budgetary matters", to "be notified to the Management Board without undue delay" (Art. 19(7))

Ⓓ

Executive Board → Executive Director

• Provision of assistance and advice to the Executive Director "in implementing the decisions of the Management Board on administrative and budgetary matters pursuant to Article 20" ("without prejudice to the responsibilities of the Executive Director set out in Article 20", Art. 19(2), point (c))

Executive Director → Executive Board

• Participation in Executive Board meetings without the right to vote (Art. 19(3))

Ⓔ

Management Board → National Liaison Officers Network

• Establishment of the National Liaison Officers Network (Art. 23(1))

Ⓕ

Executive Director → Advisory Group

• Chairperson of ENISA Advisory Group (or "by any person whom the Executive Director appoints on a case-by-case basis") (Art. 21(3))

Advisory Group → Executive Director

• Provision of "particular advi[c]e [...] on the drawing up of a proposal for ENISA's annual work programme, and on ensuring communication with the relevant stakeholders on issues related to the annual work programme" (Art. 21(5))

Ⓖ

Executive Director → Ad Hoc Working Groups

• Establishment of ad hoc working groups "where necessary and within ENISA's objectives" and appointment of member experts (Art. 20(4))

Other connections

"ENISA" → Management Board

• Report to Management Board "on the outcome" of ENISA's involvement in international exercises (Art. 12, point (a))

• Provision of Management Board secretariat (Art. 17(6))

"ENISA" → European Commission

• Transmission of ENISA's final accounts "together with the Management Board's opinion" "by 1 July of year N + 1" by ENISA's accounting officer to the Commission's accounting officer (Art. 31(7))

• Upon request of Commission, preparation of "a candidate scheme or to review an existing European cybersecurity certification scheme on the basis of the Union rolling work programme" (Art. 48(1))

• Assistance of the Commission "by means of advice, opinions and analyses regarding all Union matters related to policy and law development, updates and reviews in the field of cybersecurity and sector-specific aspects thereof in order to enhance the relevance of Union policies and laws with a cybersecurity dimension and to enable consistency in the implementation of those policies and laws at national level" (recital (22))

"ENISA" → European Parliament

• Transmission of ENISA's final accounts "together with the Management Board's opinion" "by 1 July of year N + 1" by ENISA's accounting officer (Art. 31(7))

"ENISA" → Council

• Transmission of ENISA's final accounts "together with the Management Board's opinion" "by 1 July of year N + 1" by ENISA's accounting officer (Art. 31(7))

"ENISA" → Court of Auditors

• Transmission of ENISA's final accounts "together with the Management Board's opinion" "by 1 July of year N + 1" by ENISA's accounting officer (Art. 31(7))

European Commission → "ENISA"

• Every five years, evaluation of "the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need to modify ENISA's mandate and the financial implications of any such modification" (Art. 67(1))

• Right to "propose that this Regulation [the CSA] be amended with regard to the provisions related to ENISA" when "the Commission considers that the continued operation of ENISA is no longer justified in light of the objectives, mandate and tasks assigned to it" (Art. 67(1))

Council → "ENISA"

• Responsibility for "authori[zing] the appropriations for the contribution from the Union to ENISA" (with European Parliament) (Art. 29(5))

• Responsibility for adoption of ENISA's establishment plan (with European Parliament) (Art. 29(6))

Parliament → "ENISA"

• Responsibility for "authori[zing] the appropriations for the contribution from the Union to ENISA" (with Council) (Art. 29(5))

• Responsibility for adoption of ENISA's establishment plan (with Council) (Art. 29(6))

European Commission → Parliament

• Submission of "estimates it [Commission] deems to be necessary for the [ENISA's] establishment plan and the amount of the contribution to be charged to the general budget of the Union" (Art. 29(4))

• Transmission of "a report on the evaluation of ENISA [Art. 67(1)] together with its conclusions" (Art. 67(4))

European Commission → Council

• Submission of "estimates it [Commission] deems to be necessary for the [ENISA's] establishment plan and the amount of the contribution to be charged to the general budget of the Union" (Art. 29(4))

• Transmission of "a report on the evaluation of ENISA [Art. 67(1)] together with its conclusions" (Art. 67(4))

ENISA's actor-network derived from relevant EU legislation

Actor Group		Actor	Legislation	
EUIBAs and EU-Internal Coordination Bodies	EU Institutions	Union institutions	Cybersecurity Act	***Policy*** Art. 6(1), point (f)
		European Commission	Cybersecurity Act	***International cooperation*** Art. 12, point (b)) Art. 12, point (c)) Art. 12, point (d))
			NIS 2 Directive	***Policy*** Art. 3(4) Art. 4(3) Art. 21(5) Art. 22(2)
			Regulation 2024/1789	***Policy*** Art. 8a(3)
			Cyber Resilience Act	***Policy*** Art. 14(9) Art. 14(10) Art. 56(2) Art. 70(2) ***Expertise*** Art. 56(3) Art. 57(7) ***Cooperation*** Art. 16(4) Art. 60(3)
			Electronic Communications Code	***Policy*** Art. 40(5)
			Cyber Solidarity Act	***Policy*** Art. 12(4) Art. 14(7) Art. 19(2) Art. 19(11) ***Cooperation*** Art. 14(5) Art. 16(4) Art. 16(10)
		European Central Bank (ECB)	Digital Operational Resilience Act	***Cooperation*** Art. 19(7)

	EU Bodies	European Data Protection Supervisor (EDPS)[192]	⬚⬚ Cybersecurity Act	***Cooperation*** Art. 7(2)
	EU Agencies	European Union Agency for the Cooperation of Energy Regulators (ACER)	⬚⬚ Network Code	***Policy*** Art. 8(3) Art. 47(7) Art. 12(1) Art. 42(4) ***Expertise*** Art. 12(3) Art. 12(5) Art. 13(1) ***Cooperation*** Art. 41(1)
		European Supervisory Authorities (ESAs)	⬚⬚ Digital Operational Resilience Act	***Expertise*** Art. 21(1) ***Cooperation*** Art. 19(7) Art. 34(3) Art. 49(1) Art. 32(4), point (c)) ***Certification and standardization*** Art. 15 Art. 16(3) Art. 18(3) Art. 18(4) Art. 20
			⬚⬚ Directive on Payment Services (2015/2366)	***Cooperation*** Art. 95(5)
		European Cybersecurity Competence Centre (ECCC)	⬚⬚ Regulation 2021/887	***Cooperation*** Art. 12(7) Art. 18(5) ***Research and innovation*** Art. 3(2) Art. 5(2), point (c) Art. 10(1) Art. 13(4)
			⬚⬚ Cyber Solidarity Act	***Expertise*** Art. 9(4)
		European Union Agency for the Operational Management of Large-Scale IT Systems in the	⬚⬚ Regulation 2018/1726	***Expertise*** Art. 41(3)

		Area of Freedom, Security and Justice (eu-LISA)		
		European Union Agency for Law Enforcement Cooperation (Europol) & European Cybercrime Centre (EC3)	◆◆ Cybersecurity Act	***Cooperation*** Art. 7(2)
	EU Interinstitutional Services	Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU)	◆◆ Cybersecurity Act	***Capacity*** Art. 6(1), point (g) ***Cooperation*** Art. 7(2) Art. 13(3), point (e) Art. 13(7) Art. 22(2) Art. 22(3) Art. 13(5) Art. 21(8)
			◆◆ Regulation 2023/2841	***Expertise*** Art. 13(5) ***Capacity*** Art. 13(5)
	EU-internal Coordination Bodies	Interinstitutional Cybersecurity Board (IICB)	◆◆ Regulation 2023/2841	***Policy*** Art. 5(1) ***Cooperation*** Art. 10(3), point (a)(xiii) Art. 11, point (o) Art. 23(1)
Union-Level Cooperation and EU-Member State-Coordination Bodies	NIS Cooperation Group	◆◆ Cybersecurity Act	***Cooperation*** Art. 5(4) | Art. 6(1), point (j) | Art. 14(3)	
		◆◆ NIS 2 Directive	***Policy*** Art. 19(1) | Art. 19(5) | Art. 19(6) ***Expertise*** Art. 22(1) | Art. 23(9)	
		◆◆ Cyber Resilience Act	***Expertise*** Art. 17(3)	
		◆◆ Cyber	***Policy***	

192 See also European Data Protection Supervisor (2022): Pairing up Cybersecurity and Data Protection efforts: EDPS and ENISA sign Memorandum of Understanding.

		Solidarity Act	Art. 12(6)
	European Data Protection Board	◆◆ Cybersecurity Act	***Policy*** Art. 5(5)
	European Data Innovation Board	◆◆ Data Governance Act	***Policy*** Art. 29(1)
	CSIRTs Network	◆◆ Cybersecurity Act	***Cooperation*** Art. 7(3) | Art. 7(4) | Art. 7(7), point (b)
		◆◆ NIS 2 Directive	***Expertise*** Art. 23(9) ***Cooperation*** Art. 15(2)
		◆◆ Cyber Resilience Act	***Cooperation*** Art. 16(4)
	European cyber crisis liaison organisation network (EU-CyCLONe)	◆◆ NIS 2 Directive	***Cooperation*** Art. 16(2)
		◆◆ Cyber Resilience Act	***Cooperation*** Art. 17(1)
	European Digital Identity Cooperation Group	◆◆ eIDAS Regulation	***Cooperation*** Art. 46e(4) | Art. 46e(5), point (c)(iv)
	Interoperable Europe Board	◆◆ Interoperable Europe Act	***Cooperation*** Art. 15(3)
	European Cybersecurity Certification Group (ECCG)	◆◆ Cybersecurity Act	***Certification and standardization*** Art. 8(1), point (e) | Art. 62
	DORA Oversight Forum	◆◆ Digital Operational Resilience Act	***Cooperation*** Art. 32(4), point (c)
Member States	Cyber Resilience Act designated market surveillance authorities	◆◆ Cyber Resilience Act	***Policy*** Art. 52(5) | Art. 52(10) ***Expertise*** Art. 52(5)
	Network Code competent authorities	◆◆ Network Code	***Policy*** Art. 4(3) ***Capacity*** Art. 42(1) ***Cooperation*** Art. 37(1), point (g)
	National CSIRTs	◆◆ Cybersecurity	***Capacity*** Art. 6(1), point (g)

		Act	
		◆◆ Network Code	***Cooperation*** Art. 37(2), point (a)
		◆◆ Cyber Resilience Act	***Cooperation*** Art. 16(2) | Art. 17(2)
	Electronic Communications Code competent authorities	◆◆ Electronic Communications Code	***Cooperation*** Art. 40(2)
	Single Point of Contact (SPOC)	◆◆ NIS 2 Directive	***Cooperation*** Art. 8(4) | Art. 23(9) | Art. 27(4)
	NIS 2 cyber crisis management authorities and CSIRTs	◆◆ Cyber Solidarity Act	***Cooperation*** Art. 16(9)
	Single point of contact for trust services, European Digital Identity Wallets and notified electronic identification schemes	◆◆ eIDAS Regulation	***Cooperation*** Art. 46c(2)
	Certification body[193]	◆◆ Commission Implementing Regulation 2024/482	***Certification and standardization*** Art. 10(5) | Art. 14(2) | Art. 30(5) | Art. 42(3)
	National cybersecurity certification authority	◆◆ Commission Implementing Regulation 2024/482	***Certification and standardization*** Art. 23(4) | Art. 38(1) | Art. 42(3)
Non-State Stakeholders and Bodies With Stakeholder Involvement	AI Act Advisory Forum	◆◆ Artificial Intelligence Act, 2024/1689	***Cooperation*** Art. 67(5)
	ENTSO for Electricity and the EU DSO entity	◆◆ Network Code	***Policy*** Art. 16(1), point (n) | Art. 16(3) | Art. 19(5) ***Expertise*** Art. 37(9) | Art. 48(9) ***Cooperation*** Art. 43(5) | Art. 44(6) | Art. 45(2) ***Certification and standardization*** Art. 48(8)
	Public	◆◆ Cybersecurity	***Expertise*** Art. 9, point (d)

		Act	***Capacity*** Art. 10, point (a)
	"Citizens, organisations and businesses (across the Union)"	◆◆ Cybersecurity Act	***Expertise*** Art. 9, point (e) ***Capacity*** Art. 10, point (a)
	High- and critical-impact entities	◆◆ Network Code	***Expertise*** Art. 38(2) ***Cooperation*** Art. 45(2) | Art. 38(2)
	Transmission system operators (TSOs)	◆◆ Network Code	***Expertise*** Art. 9(1) | Art. 34(1) | Art. 34(3) | Art. 36(2)
	Sectoral entities	◆◆ Cybersecurity Act	***Cooperation*** Art. 6(2)
	Manufacturers	◆◆ Cyber Resilience Act	***Cooperation*** Art. 14(1) | Art. 14(3) | Art. 15(1) | Art. 15(2) | Art. 15(3)
	Natural or legal persons	◆◆ Cyber Resilience Act	***Cooperation*** Art. 15(5) | Art. 15(1) | Art. 15(2) | Art. 15(3)
	Certification body[194]	◆◆ Commission Implementing Regulation 2024/482	***Certification and standardization*** Art. 10(5) | Art. 14(2) | Art. 30(5) | Art. 42(3)
	Stakeholder Cybersecurity Certification Group (SCCG)	◆◆ Cybersecurity Act	***Certification and standardization*** Art. 8(2) | Art. 22(4) | Art. 22(2)

ENISA's budget requests vs. budget allocations

This table provides an overview of the development of ENISA's human and financial resources from 2014 to 2025. By comparing ENISA's budget requests with its actual resource allocation, it highlights the gap between these figures (columns one and three). Additionally, the table illustrates how resource allocation in a given year compares to the budget from the previous year, showing any differences or indicating continuity (columns two and four). The sources for the respective budget

193 Certification bodies can be private entities or be run by Member States.
194 Certification bodies can be private entities or be run by Member States.

years are as follows: 2025, 2024, 2023, 2022, 2021, 2020, 2019, 2018, 2017, 2016, 2015, and 2014.

For clarity, the following symbols in columns one and three represent specific budget outcomes:

▼ indicates that ENISA received less than it requested,

▶ indicates that ENISA's request was fully met, meaning it received the exact resource adjustment it sought,

▲ indicates that ENISA's resource allocation exceeded its request.

To illustrate how the table should be read, take the 2025 budget year as an example: ENISA requested six additional temporary posts and a budget increase of approximately €4.26 million. Ultimately, the European Commission granted one additional temporary post and one additional seconded national expert (SNE). Compared to its request, this resulted in a shortfall of five temporary posts but an increase of one SNE (= ▼). The approved budget increase was €795.700, which was €3.47 million less than ENISA's original request (= ▼)

Budget Year	Delta: Human Resources	Compared to the previous budget: What did ENISA end up getting?	Delta: Financial Resources	Compared to the previous budget: What did ENISA end up getting?
2025	▼ *Minus*: 5 FTEs (- 5 TA) *Plus*: 1 FTE (+ 1 SNE)	+ 2 FTEs (+ 1 TA and 1 SNE)	▼ *Minus*: 3.47 million euros	+ 795.7 thousand euros
2024	▼ *Minus*: 17.5 FTEs	No adjustment	▼ *Minus*: 8.27 million euros	+ 492.5 thousand euros
2023	▶ *Minus/Plus*: 0	+ 2 FTEs (+ 2 SNEs)	▶ *Minus/ Plus*: 0	+ 1.5 million euros
2022	*Delta unclear*	+ 8 FTEs (+ 6 new establishment plan posts & 2 CA)	▲ *Plus*: 610 thousand euros	+ 745 thousand euros
2021	▶ *Minus/Plus*: 0	+ 7 FTEs (+ 7 new establishment plan posts)	▶ *Minus/ Plus*: 0	+ 1.63 million euros
2020	▶	+	▶	+

	Minus/Plus: 0	19 FTEs (+ 10 new establishment plan posts, 3 CA & 6 SNEs)	*Minus/ Plus*: 0	4.85 million euros
2019	▶ *Minus/Plus*: 0	+ 5 FTEs (+ 12 new establishment posts, - 3 CA & - 4 SNE)	▼ *Minus*: 1.1 million euros	+ 5 million euros
2018	▼ *Minus*: 7 FTE (- 6 temporary agents, - 1 establishment plan post)	- 1 FTE (- 1 establishment plan post)	▼ *Minus*: 2.86 million euros	+ 180.2 thousand euros
2017	▼ *Minus*: 25 FTEs (- 25 temporary agents) *Plus*: 7 FTEs (- 7 SNEs)	+ 7 FTEs (+ 7 SNEs)	▼ *Minus*: 5.1 million euros	+ 184.1 thousand euros
2016	▼ *Minus*: 5 FTEs (- 5 establishment plan posts)	+ 9 FTEs (+ 9 contract agents)	▼ *Minus*: 695 thousand euros	+ 964.6 thousand euros
2015	▶ *Minus/Plus*: 0	+ 7 FTEs (+ 7 new posts & conversion of 2 already existing SNE posts to 2 CNA posts)	▼ *Minus*: 280 thousand euros	+ 346 thousand euros
2014	▼ *Minus*: 1 FTE (- 1 additional establishment post)	+ 1 FTE (+ 1 additional establishment plan post)	▼ *Minus*: 2.48 million euros	+ 441 thousand euros

List of abbreviations

Abbreviation	Full Name
ACER	European Union Agency for the Cooperation of Energy Regulators
APT	Advanced Persistent Threat
BEREC Office	Agency for Support for BEREC (Body of European Regulators for Electronic Communications)
CEN	European Committee for Standardization

CENELEC	European Committee for Electrotechnical Standardization
CEPOL	European Union Agency for Law Enforcement Training
CERT-EU	Cybersecurity Service for the Union institutions, bodies, offices and agencies
CFSP	Common Foreign and Security Policy
CIISI-EU	Cyber Information and Intelligence Sharing Initiative
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRTs	Computer Security Incident Response Teams
CSIRTs Network	Computer Security Incident Response Teams Network
CSOA	Cyber Solidarity Act
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DG DIGIT	Directorate-General for Digital Services
EASA	European Union Aviation Safety Agency
EBA	European Banking Authority
EC3	European Cybercrime Centre
ECA	European Court of Auditors
ECASEC	European Competent Authorities for Secure Electronic Communications Expert Group
ECATS	European Competent Authorities for Trust Services Expert Group
ECB	European Central Bank
ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
ECCSA	European Centre for Cybersecurity in Aviation
ECRB	Euro Cyber Resilience Board for pan-European Financial Infrastructures
ECRG	Electronic Communications Reference Group
ECSF	European Cybersecurity Skills Framework
EDA	European Defence Agency
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EIOPA	European Insurance and Occupational Pensions Authority
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Cybersecurity

ERA	European Union Agency for Railways
ESAs	European Supervisory Authorities
ESDC	European Security and Defence College
ESMA	European Securities and Markets Authority
ESOs	European Standards Organisations
ETSI	European Telecommunications Standards Institute
EU INTCEN	European Union Intelligence and Situation Centre
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
EU-JCAR	EU Joint Cyber Assessment Reports
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
EUAN	EU Agencies Network
EUCC	EU Common Criteria
EUCS	European Union Cloud Services Scheme
EUIBAs	EU Institutions, Bodies and Agencies
EURATOM	European Atomic Energy Community
Eurocontrol	European Organisation for the Safety of Air Navigation
Europol	European Union Agency for Law Enforcement Cooperation
EuroSCSIE	European SCADA and Control Systems Information Exchange
EUSPA	European Union Agency for the Space Programme
FIRST	Forum of Incident Response and Security Teams
FRA	European Union Agency for Fundamental Rights
FTEs	Full-Time Equivalents
HWPCI	Horizontal Working Party on Cyber Issues
IICB	Interinstitutional Cybersecurity Board
ISACs	Information Sharing & Analysis Centers
ISO	International Organization for Standardization
ITI	Information Technology Industry Council
ITU	International Telecommunication Union
MEPs	Members of the European Parliament
MFF	Multiannual Financial Framework
NIS	Directive concerning measures for a high common level of security of network and information systems across the Union (2016)
NIS 2	Directive on measures for a high common level of cybersecurity across the

	Union (2022)
NLO	National Liaison Officers Network
OECD	Organisation for Economic Co-operation and Development
R&D	Research and Development
SCCG	Stakeholder Cybersecurity Certification Group
SNE	Seconded National Expert
SOCs	Security Operation Centres
SPD	Single Programming Document
SPOC	Single Point of Contact
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TSOs	Transmission System Operators

Acknowledgement

This analysis was supported by interviews with researchers and practitioners, as well as online collaboration, including with representatives from EU Member States, industry, academia, and civil society. Inspiration for this paper was drawn from a workshop conducted in June 2024 on 'Facilitating National Implementation and Application of EU Cybersecurity Policy,' as well as from conversations on national approaches to implementing EU cybersecurity legislation and policies. The author would like to thank the involved subject matter experts for their insights and for sharing their experience.

At interface, the author would particularly like to thank Sven Herpig for input and advice in turning the initial idea into this policy paper, Jasen Ho for research support, Luisa Seeling for support in editing the text, Alina Siebert for layouting the paper and designing the paper's visuals, Helene Pleil for feedback on a first draft, Sebastian Rieger and Ernesto Oyarbide-Magaña for helping to spread the word about this publication, and Frederic Dutke for support in implementing the workshop.

Research and analysis have not been commissioned by any entity. Designated programme funds from interface's Cybersecurity Policy and Resilience programme were used to fund this work.

Author

Christina Rupp
Senior Policy Researcher Cybersecurity Policy and Resilience
crupp@interface-eu.org
+49308145037880

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
Ebertstraße 2
D-10117 Berlin

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com