DIGITALEUROPE

15 SEPTEMBER 2023

Adapting ENISA's mandate and collaboration in a changing cyber landscape

Executive summary

The upcoming evaluation of the European Union Agency for Cybersecurity (ENISA) is crucial to assess its performance and explore potential modifications to its mandate, considering its role in the evolving cybersecurity landscape.[1]

ENISA has been successful in promoting network and information security across Europe, but must adapt to address emerging cyber threats and the changing cybersecurity environment. It now faces expanded responsibilities due to new legislative acts, including the new Directive on measures for a high common level of cybersecurity across the Union (NIS2) and the Cyber Resilience Act.[2]

Expanding ENISA's mandate presents several challenges, including the predominant competence of Member States in national security matters, the diversity in legal frameworks and expertise amongst Member States, and resource allocation constraints.

To enhance the effectiveness of both ENISA and the European cybersecurity certification framework, we suggest various lines of action and reforms:

- ENISA should **further foster coordination and cooperation** amongst Member States, facilitating information sharing, best practice dissemination, and harmonisation of cybersecurity policies. It should deepen its sector-specific expertise, prioritising critical sectors and assets and collaborating with sector-specific authorities and organisations, such as information sharing and analysis centres (ISACs);

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13919-European-Union-Agency-for-Cybersecurity-and-EU-cybersecurity-certification-framework-evaluation_en.

[2] Directive (EU) 2022/2555 and COM(2022) 454 final, respectively.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- ENISA should play a more prominent role in **advising on planned EU legislative initiatives** with cybersecurity implications, enhancing the coherence and impact of cybersecurity policymaking in the EU;
- ENISA's **tasks** within the EU's cybersecurity ecosystem should be **further clarified to avoid duplication and ensure efficient resource allocation across the EU**. Structured collaboration with the European Cybersecurity Competence Centre (ECCC) and strengthening support to existing bodies like the NIS Cooperation Group, the CSIRTs Network and EU-CyCLONe can streamline ENISA's role;
- Collaboration between the public and private sectors is essential to enhance Europe's resilience against cyber threats. A **Joint Public-Private Expert Unit**, comprising chief information security officers (CISOs) and leading companies operating in Europe, should be considered to advise on strategies and measures for proactive threat mitigation;
- To improve the effectiveness of the European cybersecurity certification framework, an **evidence-based approach** should be adopted, including expert-driven impact assessments. The Union Rolling Work Programme (URWP) should be published promptly to provide stakeholders with foresight on upcoming schemes; and
- The **Stakeholder Cybersecurity Certification Group (SCCG) should be empowered to play a more proactive role** by providing non-binding opinions, participating in impact assessments, interacting with the European Cybersecurity Certification Group (ECCG), and promoting enhanced meeting dynamics.

ENISA's evaluation and adaptation are essential to meet the evolving cybersecurity challenges facing Europe. Expanding its mandate, whilst respecting Member States' competencies, can be achieved through a multifaceted approach and effective resource allocation. ENISA should collaborate with existing EU bodies, contribute to policymaking, and foster public-private cooperation to strengthen Europe's cybersecurity resilience.

Table of contents

Evaluation of ENISA

ENISA has been operating successfully for almost two decades, playing a central role in improving network and information security across Europe. ENISA's current mandate is primarily focused on providing guidance, expertise and support. Its efforts in promoting best practices and facilitating cooperation amongst Member States have played a pivotal role in advancing cybersecurity within the EU.

ENISA's mandate must now further evolve to address emerging cyber threats and the changing cybersecurity landscape. Importantly, ENISA's mandate needs to reflect its exponential role as introduced in recently, or soon to be, adopted legislation, alongside efforts by national competent authorities to supervise implementation and enforcement.

ENISA is required to play an important role in the implementation of the new NIS2 Directive, and potentially contribute significantly to the oversight and enforcement of the proposed Cyber Resilience Act. In addition to the development of certification schemes under the Cybersecurity Act, ENISA will also be involved in supporting the upcoming AI Act, the Digital Operational Resilience Act (DORA) and the new eIDAS Regulation.[3]

The Agency's mission has shifted from a time when cybersecurity was a relatively peripheral concern for companies and authorities alike, towards a situation where the very existence and wellbeing of Europe's economy and society depend on heightened cyber awareness and response.

This shifting paradigm necessitates increased action at the European level. ENISA's current design and resource allocation are no longer fully suitable to address the current environment effectively.

An expansion of ENISA's mandate encounters challenges rooted in the EU treaties and Member States' competence over security matters. In this context, it is essential to explore how ENISA's role can be reformed to overcome these challenges, and to effectively respond to growing cyber threats both within the EU and on the international stage.

Challenges of expanding ENISA's mandate

Expanding ENISA's mandate to address an increasingly complex threat landscape encounters several hurdles, including:

- The EU treaties grant Member States predominant competence over security matters. This means that significant aspects of cybersecurity, particularly those related to national security and defence, fall squarely

[3] COM(2021) 206 final, Regulation (EU) 2022/2554 and COM(2023) 209 final, respectively.

within the purview of individual Member States. ENISA must navigate this whilst extending its role in cybersecurity;

- Despite harmonisation efforts, there is still huge diversity in Member States' legal frameworks and expertise for cybersecurity, further complicating ENISA's mission. ENISA's expanded role requires aligning with these varied national situations; and
- Resource allocation: Expanding ENISA's mandate necessitates adequate resources. Achieving this amidst budgetary constraints, competing priorities for the EU budget, and an acute cyber skills shortage is a significant challenge.[4]

Updating ENISA's design and resource allocation

To effectively address emerging developments and risks in the evolving cybersecurity landscape, ENISA can undergo specific reforms:

- **Enhanced coordination**: ENISA can foster even greater coordination and cooperation amongst Member States. Whilst the EU treaties preserve Member States' competence, ENISA can strengthen its role as a facilitator for collaboration through better information sharing, best practice dissemination and harmonisation of cybersecurity policies;
- **Sectoral expertise**: ENISA should deepen its sector-specific expertise to provide tailored guidance and support to critical sectors, by adopting a risk-based approach that identifies and prioritises critical assets and sectors. This approach would allow ENISA to concentrate its efforts on areas where the potential impact of cyber threats is highest. Collaboration with sector-specific authorities and organisations, such as ISACs, must be strengthened to help identify and remedy sector-specific threats and vulnerabilities;
- **International cooperation**: Acknowledging the global nature of cyber threats, ENISA should enhance its international cooperation efforts. This entails collaborating with like-minded partners in third countries, international organisations and cybersecurity agencies to develop a cohesive response to cyber threats that transcends national borders; and
- **Resource allocation and funding**: Adequate resource allocation is essential for ENISA's success. It is crucial to secure sufficient funding, personnel and expertise to fulfil an expanded mandate effectively. This requires increased budgetary allocations within the EU framework. We welcome the intention, as reflected in the proposed Cyber Solidarity

[4] Current estimates put the global cybersecurity workforce gap at 3.4 million people, with Europe lacking more than 200,000 cyber professionals. See the 2021 and 2022 ISC2 Cybersecurity Workforce Studies, available at https://www.isc2.org/research.

Act,[5] to reinforce ENISA through additional funding to reinforce Europe's capacity to respond to major cyber incidents. This resource allocation should take into consideration the foreseen work plan for at least five years. ENISA should work in collaboration with EU institutions and bodies to identify areas where funding can have the most significant impact in enhancing Europe's cybersecurity resilience.

Circumventing challenges through multifaceted approaches

Whilst challenges exist due to Member States' competence over security, they can be circumvented through multifaceted approaches:

- **Gradual expansion**: ENISA's mandate expansion can be gradual, focusing initially on areas where cooperation is more straightforward and expanding progressively into more complex domains. This approach respects the existing legal framework and would ensure that ENISA's expanded efforts are targeted and outcomes are measurable;
- **Complementary roles**: ENISA should continue to position itself as a complementary actor, increasing its support to Member States in areas where EU-wide collaboration is beneficial. This approach respects the EU treaties whilst fostering cooperation; and
- **Consensus building**: Achieving consensus amongst Member States is paramount. ENISA should play an enhanced role in facilitating dialogue, sharing best practices and demonstrating the added value of its involvement in cybersecurity.

Consistency in EU policy

ENISA should play a more prominent role in shaping and influencing Union policies related to cybersecurity. Granting ENISA a more explicit power to be consulted and provide Opinions on planned EU legislative initiatives related to cybersecurity is crucial to ensure more effective policymaking going forward. ENISA needs to function as an independent watchdog that critically scrutinises EU policy to ensure it promotes cybersecurity.

An obligation should be introduced for the European Commission to consult ENISA when drafting legislative proposals with cybersecurity implications. In preparing its Opinions, ENISA should engage with a wide range of stakeholders, including industry, civil society organisations and academia.

Mandatory ENISA consultation on legislative initiatives related to cybersecurity would contribute to more effective and comprehensive cybersecurity policies, ultimately enhancing the EU's digital resilience.

[5].

Relationship with other EU bodies

In light of the complex network of players in the EU cyber ecosystem, a review of ENISA's mandate should establish clearer delineations of responsibilities to foster collaboration amongst various actors. Refining ENISA's role within the EU's cybersecurity ecosystem is essential to ensure that resources are effectively allocated, tasks are not duplicated, and the EU's cybersecurity objectives are met efficiently.

To this end, the review should:

- **Focus on core functions**: ENISA should concentrate on its core functions. This means avoiding tasks that can be better managed by other EU institutions or Member States. The objective is to prevent redundancy and ensure that ENISA's efforts are directed where they can make the most significant impact;
- **Collaboration with the European Cybersecurity Competence Centre (ECCC)**: The newly established ECCC in Bucharest is a pivotal player in advancing cybersecurity research, innovation and development. A new mandate should enable close ENISA collaboration with the ECCC, ensuring alignment with its research and innovation activities. This collaboration can involve sharing insights on emerging threats, coordinating research efforts, and jointly developing innovative cybersecurity solutions;
- **Leveraging existing bodies**: ENISA's role in supporting existing EU bodies and structures, such as the NIS Cooperation Group, the CSIRTs Network and EU-CyCLONe, further improving information sharing, joint initiatives and coordinated efforts to avoid duplication and ensure synergies; and
- **Regular evaluation**: To ensure the effectiveness of ENISA's mandate, regular evaluations should be conducted to assess the impact of ENISA's consultative role, the avoidance of task duplication, and the overall coordination within the EU's cybersecurity ecosystem. Adjustments can be made based on the outcomes of these evaluations to fine-tune ENISA's role further.

By adopting these recommendations, ENISA can contribute to a more streamlined and efficient EU cybersecurity governance model. Collaboration and coordination amongst various EU bodies and institutions will be instrumental in addressing emerging cyber threats and strengthening Europe's overall cybersecurity resilience.

Joint public-private cooperation

Europe's resilience depends heavily on the extent to which the public and private sectors can cooperate to provide agile responses to cyber threats and to adopt state-of-the-art cybersecurity solutions.

DIGITALEUROPE has called for a Joint Public-Private Expert Unit to advise on skills, cooperation and preparedness prior to an attack.[6] This Expert Unit, which should be considered for ENISA's review and new mandate, can advise on strategies and measures to proactively mitigate cyber threats. The Expert Unit should comprise CISOs and leading companies operating in Europe, but not limited to EU-headquartered entities.

This collaborative approach will not only enhance resilience but also promote a secure internal market through effective public-private partnership. Regular evaluation and measurement of outcomes will ensure that the partnership remains impactful and adaptable.

Effectiveness of the European cybersecurity certification framework

DIGITALEUROPE has supported and been actively participating in the development and implementation of the cybersecurity certification framework.

The importance of taking measures to ensure the cybersecurity of our businesses, services and products has only increased since the Cybersecurity Act was adopted. Despite significant efforts, none of the schemes currently under development has been adopted yet. We believe these delays can be remedied by removing existing bottlenecks in the process, as elaborated below.

Adopting an evidence-based approach

An expert-driven impact assessment is crucial before developing certification schemes. This assessment should evaluate the potential effects of certification schemes on the EU as a whole and on specific sectors. By adopting an evidence-based approach, we can avoid unnecessary delays and ensure that schemes are developed with a clear understanding of their implications.

The politicisation of schemes, such as the draft European Cybersecurity Certification Scheme for Cloud Services (EUCS), has significantly delayed the development of the schemes and hampered overall trust in the framework. We recommend that any political requirements being considered for certification schemes should undergo proper political discussion within the legislative process, following an expert impact assessment. This would ensure that political considerations do not unduly delay the certification framework.

---

[6] See DIGITALEUROPE, *The digital front line: 15 actions to boost Europe's digital resilience*, available at https://www.digitaleurope.org/resources/the-digital-front-line-15-actions-to-boost-europes-digital-resilience/

Finally, we note that the EUCS, the 5G Cybersecurity Certification scheme (EU5G) and the EU Common Criteria scheme (EUCC) have been requested directly by the Commission. This has reduced the relevance of the URWP. DIGITALEUROPE suggests conducting a comprehensive gap analysis to identify the certifications that are genuinely needed. This will prevent schemes from being introduced without a clear need or rationale.

Union Rolling Work Programme

The URWP should be the central tool to provide industry, national authorities and standardisation bodies with the necessary foresight regarding the resources and expertise that must be put into the development and adoption of European cybersecurity certification schemes. This strategic document allows stakeholders to prepare for upcoming schemes, ensuring a smoother and more coordinated certification process.

The EU Cybersecurity Strategy stated that the URWP should be adopted in early 2021 and updated at least once every three years.[7] Regrettably, the first URWP has yet to be published.

The growing number of legislative files considering certification schemes as compliance tools has created an urgent need to have a clear work programme to be able to foresee which schemes will be developed for EU or Member State legislation. The existence of the URWP is also essential for ENISA to better coordinate its work and project budgetary needs.

We urge the Commission to accelerate the process and work with the ECCG and the SCCG for the publication of the first URWP within the first half of 2024.

Ensuring a transparent process

To enhance transparency, we recommend making the **latest developments in certification schemes easily accessible** to all stakeholders. This includes providing up-to-date details on the progress and status of schemes, including the new draft EUCS, the EU5G and the EUCC. Transparency promotes trust and stakeholder buy-in.

We emphasise the need for **regular public consultations** throughout the development of certification schemes. Most notably, no public consultations have been conducted on considerably revised versions of the EUCS since the first consultation in 2020, leaving affected stakeholders unable to provide proper feedback.

Furthermore, the review of the cybersecurity certification framework should strengthen the requirement for schemes to be **based on existing or newly**

[7] JOIN(2020) 18 final.

developed standards, as the standards development process allows for participation of all stakeholders, and therefore ensures full transparency.

Enhancing the role of the SCCG

The Cybersecurity Act has set up both the ECCG, representing Member States, and the SCCG, representing a broad range of other stakeholders, mostly from the private sector. DIGITALEUROPE has been part of the SCCG since its creation and remains committed to its productive continuation.

We believe that the SCCG's mandatory tasks should be clarified and expanded so that the group can serve as a more proactive tool in furthering Europe's cybersecurity objectives. In particular:

- **Facilitating non-binding opinions:** To leverage the diverse perspectives within the SCCG, we propose that the group be tasked to develop its own-initiative, non-binding opinions on matters related to cybersecurity certification. The SCCG represents a broad array of stakeholders whose insights can provide a comprehensive overview of civil society's perspectives, enriching the development process;
- **Role in impact assessments:** Given its unique composition and diversity of interests, the SCCG should serve as a preferential sounding board for assessing the potential impact of proposed measures on the market. It should be consulted not only on draft certification schemes but also on prospective measures related to cybersecurity certification;
- **Interaction with the ECCG:** Collaboration between the SCCG and the ECCG is essential for the comprehensive function of both groups. Whilst maintaining their distinct roles, these groups should engage in regular exchanges, such as joint meetings (at least once a year) or sessions during their respective gatherings. Sharing conclusions and insights between the two groups can ensure better informed decisions; and
- **Enhanced meeting dynamics:** To maximise the SCCG's effectiveness, individual members should be empowered to take a more active role by proposing discussions and deliverables. An open process for review and approval by the entire group should be established. Furthermore, ENISA and the Commission should be committed to assessing and responding to the input provided by SCCG and its individual members.

FOR MORE INFORMATION, PLEASE CONTACT:

Zoey Stambolliu

Senior Manager for Infrastructure and Security Policy

zoey.stambolliu@digitaleurope.org / +32 498 88 63 05

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 102 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK