INTER
INSTITUTIONAL
CYBERSECURITY
BOARD

Ref: DECISION n° IICB/24/D015

Interinstitutional Cybersecurity Board (IICB)

Annual Report 2024

The present document incorporates the annual reports due from the Interinstitutional Cybersecurity Board (IICB) respectively to the European Parliament and Council, and to the European Commission, pursuant to Articles 10(14) and 25(1) of Regulation 2023/2841.

This document was prepared by the IICB Executive Committee and, following a discussion during the IICB Meeting of 29 November 2024, submitted for approval by written procedure on 4 December 2024, and adopted with decision n° IICB/24/D015 on 18 December 2024.

INTER
INSTITUTIONAL
CYBERSECURITY
BOARD

Contents

Foreword by the IICB Chair

In an increasingly tense geopolitical environment, in which the European Union institutions, bodies, offices and agencies (Union entities) are targeted by threat actors exploiting technical or human factors to advance on their political or criminal agendas, **cybersecurity of the EU public administration is a priority**. It must be addressed through **coordinated efforts** among all Union entities, in a **comprehensive approach** focusing on preparedness and resilience.

With this objective, **Regulation 2023/2841 entered into force on 7 January 2024**, setting the framework for **cooperation** among all Union entities and with **CERT-EU**, and driving the **implementation** of the critical mission towards enhancing cybersecurity among Union entities.

The Regulation created an **Interinstitutional Cybersecurity Board (IICB)** responsible for monitoring and supporting its implementation, as well as for providing strategic direction to **CERT-EU**. The tasks of the IICB include **annual reporting** to the European Parliament, to the Council, and to the Commission on the progress achieved by Union entities regarding their obligations.

It is my privilege and honour to present the first report today, which will contribute to the **biennial report on the state of cybersecurity** in the Union as foreseen in the NIS 2 Directive, reinforcing the message that cybersecurity of the Union entities is of the utmost importance for a well-functioning European Union.

In its first year, the IICB focused on establishing its structure and ways of working, at the same time ensuring that enough attention was given to **tangible operational measures** supporting the Union entities in responding to their obligations, and to **identifying further challenges** ahead. The IICB has established its **reputation as a serious and trustworthy actor** and has set a **solid ground for the next steps** of the implementation of the Regulation, with important milestones coming in 2025.

It is now paramount to maintain the **high level of engagement**, and to **provide Union entities and CERT-EU with the necessary means** to pursue their respective missions. Ensuring a high common level of cybersecurity across all Union entities is a *conditio sine qua non* for reinforcing and sustaining their resilience and autonomy, as a cornerstone of their political credibility.

Executive Summary

Cyber threats continue to rise year after year, and the techniques used by the threat actors are increasingly sophisticated. This is confirmed by yearly threat landscape reports and, more recently, by the Niinistö report, which underlined the **need for higher preparedness** in the EU, acknowledging a widening threat landscape, which could lead to **major repercussions** in several areas.

Union entities are targeted by threat actors exploiting technical or human factors to advance on their political or criminal agendas, interfering with Union entities' engagement on the geopolitical scene. They must therefore **lead by example** and make **all the necessary efforts to prevent and protect** against incidents which could hamper the credibility, autonomy, or resilience of the EU public administration, affect the security of staff, or compromise the integrity, availability, and confidentiality of sensitive information they process. **Regulation (EU, Euratom) 2023/2841** *laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union* entered into force on 7 January 2024, creating an **Interinstitutional Cybersecurity Board (IICB)** to monitor its implementation, and extending the mandate of the **Cybersecurity Service for the institutions, bodies, offices and agencies of the Union (CERT-EU)**.

During its first year of activities, the IICB successfully focused on the **strategic and organisational aspects** of its functioning. Notably, after appointing its members, the IICB elected the Chair and Deputy Chair, set up the Executive Committee, established the Local Cybersecurity Officers Network (LCO Network) and Technical Advisory Groups (TAGs), and adopted a Multiannual Strategy to steer its activities over the period 2024 - 2029. Equally important, given the strict deadlines, the IICB devised **practical measures** towards the implementation of the Regulation and to **provide support** to Union entities. This is reflected in the three **Strategic Objectives** of the IICB's Multiannual Strategy, as well as the **adoption of the guidelines** needed by Union entities to perform their duties. This has allowed the IICB to **establish itself as a trustworthy actor**, proving its determination to find robust responses to enhance cybersecurity in the Union entities.

In parallel, under the steering of the IICB, **CERT-EU pursued its transformation to embrace its new mandate and provided tangible support** to the IICB and Union entities, by drafting the aforementioned guidelines and assisting in the Regulation's implementation by engaging with the LCO Network through dedicated workshops and sharing relevant information on its Unified Portal.

Beyond the outcomes achieved in the first year, the IICB reflected on the opportunities and challenges ahead and **identified several issues** worthy of attention to ensure that the Union entities can achieve high common levels of cybersecurity. These include the need for **investment, resources, and deeper collaboration among Union entities and with other stakeholders**. Short-term mitigation measures put forward by the IICB only confirm the need to address the challenges, and particularly the one of resources, in a long-term, sustainable manner, with the objective to **enable Union entities to remain resilient and prepared** against the threats they face and **ensure that CERT-EU can properly deliver on its extended mandate**.

To conclude, in the overall assessment of the work performed by the IICB in 2024, the **ambitious objectives set by the Regulation for this initial period have been fully met**, demonstrating a high level of dedication in overcoming the associated challenges, mostly related to the **increased workload**. For 2025, it will be paramount that **engagement at all levels**, and by different stakeholders, firmly reflects the determination to take the necessary actions to, on the one hand, implement the Regulation, and on the other, properly equip Union entities and CERT-EU with the means to do so.

Introduction

"The European Union's security environment has in many ways taken a turn for the worse in recent years. The world is more dangerous and crisis-prone".[1]

Security is a public good and cybersecurity is **a fundamental component of security in the European Union (EU)**. Indeed, cybersecurity is a pillar of many other fields, such as law enforcement, economic stability, defence, health, privacy, and education. Preparedness is therefore fundamental to protect our way of life, especially in light of the speed of change in our multifaceted environment and the evolving threats.

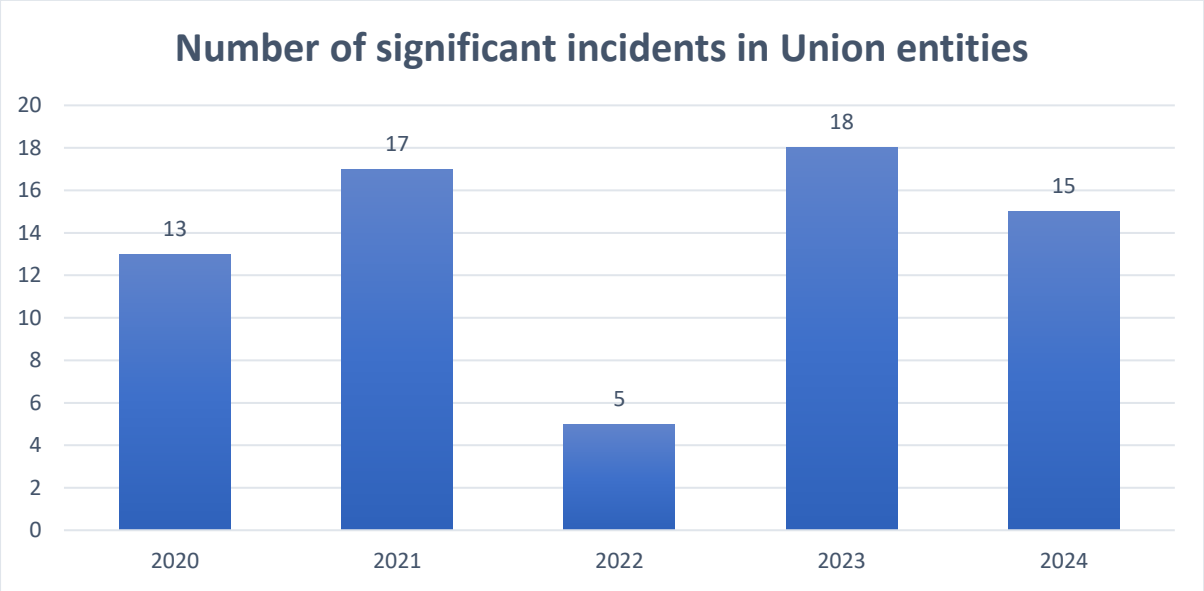
The importance of cybersecurity also lays in its role as an enabler in an increasingly digitalised world. According to a recent Eurobarometer, "*almost three-quarters of Europeans (73%) consider that the digitalisation of daily public and private services is making their life easier, including 19% who say it is making their life 'much easier'*".[2] Cybersecurity is also fundamental to ensure **high standards of privacy and protection of citizens' data**, as well as to protect information in a context of increasingly high interconnectedness between different services and Member States.

Union entities are **very attractive targets** due to their political and operational role, and the nature of the information they handle. On top of that, the sharp rise of geopolitical tensions, in our neighbourhood and globally, have led to **rapid shifts in the threat landscape**. Indeed, the European Union Agency for Cybersecurity (ENISA) Threat Landscape 2024 report[3] demonstrates that no sector is left unaffected by the adverse activities of the threat actors. Further, the CERT-EU Threat Landscape Report 2023[4] shows that the main goal of attackers targeting Union entities or their vicinity is information theft (cyberespionage), followed by hacktivism, cybercrime, information operations (exfiltration, destruction, dissemination of sensitive data) and, in a small number of cases, attacks with a destructive objective. Moreover, in 2024, a growing trend in exploitation of supply chain attacks has been observed.[5]

It should be noted that CERT-EU deals with **thousands of cyber-attacks targeting Union entities or their peers every year**, and analyses – on an annual basis – more than 600 of such attacks in detail. On this basis, CERT-EU issues approximately 180 Threat Alerts per year to Union entities, including recommendations and lines of action. This corresponds, on average, to **more than a threat alert every other business day**. This **stretches the resources of CERT-EU and Union entities thin**, as they need to look in their information and communication technology (ICT) environments for signs of malicious activities and swiftly act in case such signs are identified.

The number of **significant incidents** directly affecting Union entities also remains high, with 15 cases confirmed as of early November for 2024. These incidents require weeks and sometimes months of work to handle and recover from.

[1] Report: Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness | European Commission, p. 4.
[2] The digital decade - July 2024 - - Eurobarometer survey.
[3] ENISA Threat Landscape 2024.
[4] CERT-EU - Threat Landscape Report 2023 (europa.eu).
[5] ENISA Threat Landscape 2024.



Last but not least, **maturity levels vary broadly between Union entities**, leaving some of them extremely vulnerable to the destructive effects of cyber-attacks and requiring a lot of resources to mitigate them.

Since the beginning of 2024, CERT-EU has identified **more than 70 threat actors** targeting Union entities. When it comes to the state-sponsored actors targeting Union entities, CERT-EU has noted **two preoccupying trends**.

1) Apart from the fact that they seem to target primarily **critical infrastructure** entities, like telecommunications, energy or transport, **they do not proceed with immediate exploitation of the compromised entity**. Rather, they stay hidden in the infrastructure, waiting for the right moment to act, in a tactic called **prepositioning**.
2) The second trend is their **continuous attempts to breach in defence and diplomatic organisations**, including Union entities working in these sectors, highly likely for intelligence-gathering purposes, a trend that is on the rise since the beginning of Russia's war of aggression against Ukraine.

In conclusion, the threat level for Union entities is, beyond any reasonable doubt, **very high**. Improving the EU's **collective cybersecurity maturity and resilience** is more urgent than ever. Shifting towards more **prevention and preparedness** is also paramount, to avoid basic cyber hygiene issues and make it harder for threat actors to exploit the interconnectivity between Union entities, using less mature ones as an entry point to compromise more mature ones.

> *"Any major crisis includes unexpected elements, but the better prepared we are for anything that we can reasonably anticipate, the more capable we will be to deal with unforeseeable events".*[6]

On 7 January 2024, **Regulation (EU, Euratom) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union** (hereafter "the Regulation") entered into force. Among the tasks of the IICB, there are two specific provisions regarding annual reporting, with the first deadline on 8 January 2025:

[6] Report: Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness | European Commission, p. 7.

1. Article 10(14) states that "*the IICB shall submit a report to the European Parliament and to the Council detailing progress made with the implementation of this Regulation and specifying in particular the extent of cooperation of CERT-EU with Member State counterparts in each of the Member States".*
2. Article 25(1) states that "*the IICB, with the assistance of CERT-EU, shall report to the Commission on the implementation of this Regulation. The IICB may make recommendations to the Commission to review this Regulation.*"

In accordance with paragraph 14 of Article 10 of the Regulation, the annual report shall "*constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555".*

Considering the above, and with a view to reducing the administrative burden, this annual report covers the topics pursuant to both Articles 10 and 25 of the Regulation. As ENISA adopted its latest biennial report in September 2024, this document will constitute an input to the next one, expected in Q4 2026.

Methodology for the drafting of the report

The report draws from the lessons learnt and reflections resulting from the activities of the IICB during its first year. It refers to the documents prepared with the assistance of the IICB Secretariat, such as Decisions and summary reports, and by the Executive Committee, such as the Multiannual Strategy of the IICB for 2024 - 2029. CERT-EU contributed extensively to the parts covering more specifically its tasks and activities. Finally, the report focuses on **forward-looking challenges** resulting from the geopolitical threat landscape and associated with the organisational and administrative framework in which the Union entities operate. The actions undertaken by the IICB to address these challenges will require support through **orientations and decisions issued at the political level**.

Achievements and progress with the implementation of the Regulation in 2024

The sections below provide an overview of the achievements of the IICB during its first year of operations. Further information is available in the Annex.

1. Strategic, administrative and organisational aspects

a. IICB setup and composition

While **preparations started sooner to ensure efficiency**, the IICB was officially set up following the entry into force of the Regulation. Each Union entity listed in Article 10(3) of the Regulation designated a Member and an Alternate, including three representatives from the EU Agencies Network (EUAN). A confirmation of such appointment was sent to the Secretariat of the IICB, provided by the European Commission. During the first meeting of the IICB, its members confirmed the ad-interim Chair,[7] adopted the Rules of Procedure, and decided on the upcoming meetings for 2024. A secure portal for storing relevant documentation, such as IICB Decisions, was set up.

The Rules of Procedure of the IICB include provisions regarding the establishment of an **Executive Committee**, foreseen in the Regulation. As clarified therein, the Executive Committee "*prepares the IICB's deliberations, in particular by identifying strategic questions for consideration by the IICB, including on recommendations, guidelines, guidance and compliance measures to be issued by the IICB"*. The Executive Committee was entrusted by the IICB to prepare its Multiannual Strategy 2024 - 2029, annual report, as well as a concept paper on combined service offerings.[8]

Shortly after its creation, the IICB facilitated the establishment of the **LCO Network**, an informal group for the exchange of information and best practices related to the implementation of the Regulation. LCOs act as **single points of contact** for their Union entity and report directly to their highest level of management, further ensuring that information is communicated as necessary.

b. Decisions adopted by the IICB

Throughout 2024, the IICB adopted several Decisions to ensure not only its own **administrative functioning**, but also alignment with the **priorities** and the **deadlines** of the Regulation. In particular, this included issuance of mandatory implementation guidelines, appointing the Head of CERT-EU, and creating TAGs to support work requiring specific expertise. An overview of the most important Decisions is available in the Annex.

c. Approval of the IICB Multiannual Strategy 2024 - 2029

Article 11(c) of the Regulation states that the IICB shall **"***following a strategic discussion, adopt a multiannual strategy on raising the level of cybersecurity in the Union entities […]".* The high-level document was adopted on 6 September. It presents the mission of the IICB, sets three Strategic Objectives for the five years to come: **fostering cooperation among Union entities, providing strategic direction to CERT-EU, and elevating cybersecurity of Union entities**; and the core values that should

[7] This aimed to ensure a smooth transition from the CERT-EU Steering Board, the body preceding the IICB before the Regulation entered into force.

[8] The aim of the offerings is to 'shift left' towards more prevention and preparedness by deploying solutions that would optimise the use of resources among Union entities, while waiting for much needed reinforcements.

guide the work of the IICB and help to create a more solid interinstitutional community: **cooperation, trust, synergy, responsibility, solidarity,** and **respect for autonomy**.

d. IICB Executive Committee's Strategic Orientations for 2025

To organise, guide and prioritise its work for 2025, also with a view to enhancing predictability and planning in the implementation and monitoring of the Regulation, the Executive Committee provided the IICB with Strategic Orientations. The document recalls the **milestones** to meet for Union entities and the IICB, sets **guidance and expectations of work** in accordance with the Multiannual Strategy and outlines the planning of the activities accordingly.

2. Implementation of the Multiannual Strategy

a. Strategic Objective 1 – Fostering cooperation of Union entities on the full cybersecurity spectrum

To progress towards the accomplishment of this Strategic Objective, in 2024 the IICB reached the following targets:

i. Reporting on Technical Advisory Groups

To start the work to assist Union entities as soon as possible, the IICB set up three TAGs to assemble cybersecurity expertise: **on CERT-EU guidelines proposals, on Tools and Methodologies, and on the Human Factor**. These groups are of a technical nature and aim to help the IICB produce knowledge conducive for implementing the Regulation. They are composed of a Chair and experts from Union entities, who have committed to working towards the objectives of the TAG. Moreover, TAGs embody the transition from, and benefit from the previous network of experts of, the Cybersecurity Subgroup of the Interinstitutional Committee for Digital Transformation (ICDT CSSG).[9] More information on TAGs is available in the Annex.

ii. Set-up of mechanisms for the identification of common needs for cybersecurity solutions by Union entities with a view to propose adequate solutions

As a result of recent significant incidents which CERT-EU had to deal with, and which in one instance included the activation of the Full Cooperation Mode,[10] the Executive Committee was entrusted to **explore ways to facilitate the deployment of solutions that are secure by design, compliant with the Regulation, and designed to allow CERT-EU to efficiently deliver its services from the onset.** While the conditions under which such a concept will work are still to be defined and agreed, if supported, this **project offers a perspective** of providing a structured mechanism for all Union entities to optimise the use of their existing service capabilities, with the help of CERT-EU, and to better coordinate procurement of new services and solutions.

Furthermore, to support Union entities in accessing cybersecurity services' resources for operational support, advisory guidance and capability development, the Commission launched a procurement procedure for a new inter-institutional framework contract (MC17 FREIA[11]). This new cyber

[9] The ICDT CSSG was an informal group, predating the Regulation, set up to allow voluntary contribution of the expert communities from Union entities on specific and technical topics.
[10] The Full Cooperation Mode allows CERT-EU, among others, to request assistance on short notice from Union entities as well as establish specific communication channels to respond to a significant incident as quickly and efficiently as possible.
[11] Framework contract for the Resilience of EU Institutional Administrations.

procurement instrument, expected for Q1 2025, will allow transition from the current Cyber Security Framework Contract expiring in February 2025.

Finally, to enhance cooperation with Member States, the IICB's Multiannual Strategy includes the following, which are also the object of the guidelines on incident response coordination and cooperation for significant and major incidents:

- Set-up of a mechanism to ensure effective exchange of information, coordination, and cooperation of the Union entities in the case of major incidents, among them and where relevant with Member States, including a clear identification of the roles and responsibilities of the Union entities involved.
- Definition of coordination mechanisms and the practical modalities for exchange of information with already existing European Union cyber crisis management organisations (e.g. the type of, and modalities for, information exchange with the IICB point of contact for the European cyber crisis liaison organisation network).

b. Strategic Objective 2 – Providing strategic direction to CERT-EU and accompanying its development

To progress towards the accomplishment of this strategic objective, in 2024 the IICB reached the following targets: first, to ensure efficiency of operations, the IICB swiftly appointed the Head of CERT-EU and approved its Annual Activity Report 2023 and Work Programme 2024. Second, the IICB discussed and defined the reporting and interaction mechanisms between Union entities and CERT-EU. Third, organisational measures and communication channels to ensure the streamlining of information were set up. Additional information is provided in the Annex.

c. Strategic Objective 3 – Elevating cybersecurity posture of Union entities to the level of threat they face

To progress towards the accomplishment of this strategic objective, in 2024 the IICB reached the following targets:

i. Adoption of guidelines and recommendations based on proposals by CERT-EU

Article 5(1) of the Regulation states that "*by 8 September 2024, the [IICB] shall, after consulting [ENISA] and after receiving guidance from CERT-EU, issue guidelines to Union entities for the purpose of carrying out an initial cybersecurity review and establishing an internal cybersecurity risk-management, governance and control framework […], carrying out cybersecurity maturity assessments […], taking cybersecurity risk-management measures […], and adopting the cybersecurity plan […]*." The initial drafts were prepared by CERT-EU and submitted to an extensive review process.[12] The guidelines were subsequently adopted by the IICB on 6 September 2024, with the understanding that their revision should occur in due time and at the latest after 3 years. These documents guide Union entities through the necessary steps, with CERT-EU's support.

[12] The process included consultation of ENISA and the IICB Secretariat, the Information and Communication Technologies Advisory Committee (ICTAC), and the TAG on CERT-EU guidelines proposals. On 24 June 2024, CERT-EU updated the IICB on the status of development and the expected timeframe. On 25 June 2024, IICB Members were asked to provide their comments by 2 August 2024. CERT-EU organised several informative workshops targeted at the relevant stakeholders, notably the IICB (11 July), ICTAC (13 September), and the security officers and LCOs in the Union entities (18 September).

As foreseen in Article 21(9), on 1 July the IICB also issued a guideline, upon a proposal by CERT-EU, on Union entities' **reporting obligations on significant incidents**, as well as the voluntary notification and further ad hoc information sharing with CERT-EU.

Finally, the last mandatory guideline on **incident response coordination and cooperation** for significant and major incidents, as per Article 22(4) of the Regulation, also based on a proposal from CERT-EU, was adopted by the IICB on 29 November 2024.[13]

For the two latter guidelines, CERT-EU ensured consultations with IICB Members.

3. CERT-EU activities

a. Support for the initial cybersecurity review and establishment of the framework

Over the course of 2024, CERT-EU provided **active support and advice** to Union entities launching their initial review and building their initial plan and framework. This included, for instance, delivering several presentations and workshops, providing the possibility to discuss a Union entity's approach and to review compulsory deliverables, answering requests for clarifications, and creating a knowledge base for all Union entities. Furthermore, CERT-EU designed new features for its Unified Portal to facilitate the follow-up of cybersecurity plans by Union entities and CERT-EU. These features should be made available by 28 February 2025.

b. Cooperation with counterparts in the Member States

CERT-EU is a member of the CSIRT's Network (CNW). In 2024 it participated in all three Network's official meetings, providing updates on its work and Threat Landscape. Moreover, CERT-EU **regularly contributed** to the deliverables of all working groups of the CNW, implementing the strategic decisions of the Network in collaboration with all Member States. On more operational aspects, CERT-EU cooperated with Member States during the **EU Elections** period sharing relevant threat intelligence. What is more, CERT-EU **reported all significant incidents** to the respective national counterparts, as per the Regulation. When relevant, CERT-EU engaged in **ad hoc collaboration** for the exchange of views and best practices.

c. Full-Spectrum Adversary Approach

In 2024, CERT-EU laid down the foundations of a holistic, novel cybersecurity strategy named Full-Spectrum Adversary Approach (FSAA). The purpose of this approach is to **address the sustained high number of significant incidents** in Union entities over the last few years, **technological breakthroughs**, and the **rapid shifts in the threat landscape** by analysing threats to Union entities in all their dimensions, encompassing the growing geopolitical tensions and the digital supply-chain in all its facets. FSAA aims to develop **threat-informed, prioritised, and fit-for-purpose mitigation and detection measures** for the Union entities, supporting sound investments and concrete actions. In the next few years, this approach is expected to meaningfully support Union entities comply with the Regulation and further improve services that CERT-EU delivers to Union entities.

[13] As regards the guidelines adopted on 29 November, they followed a consultation process of IICB Members which took place between 9 and 23 October and was complemented by an information workshop for IICB representatives on 15 October.

d. General status of calls for action

CERT-EU issued a Call for Action on 5 February requesting **Union entities** to replace a number of cybersecurity products due to inadequate response to critical security issues by August 2025. CERT-EU asked the Union entities using these products to acquire forensics evidence and apply the patches provided by their vendor by 9 February 2024 at the latest. CERT-EU also asked Union entities to establish a roadmap to replace the aforementioned products and share it with CERT-EU.

e. Resources for 2024

When the Regulation was adopted in December 2023, the resources at CERT-EU were **considerably lower** than those needed for its implementation, particularly in terms of posts. Therefore, when the Regulation entered into force, CERT-EU put several non-essential services **temporarily on hold, to prioritise** drafting the proposals for the mandatory guidelines the IICB needed to issue under tight deadlines.[14] To meet those deadlines and support the extensive consultation process that was required to make the proposals befitting the very heterogenous community of Union entities, the Commission and the Parliament agreed to provide ad-hoc reinforcement to CERT-EU resources at the beginning of 2024. While not sufficient to address all its tasks under the Regulation, this reinforcement allowed CERT-EU to consult all relevant stakeholders and provide the proposals for guidelines on time. A comprehensive overview of CERT-EU's resources, revenues and expenditure will be found in CERT-EU's Annual Activity Report 2024, due in the beginning of 2025.

[14] CERT-EU opened the services that were temporarily put on hold to all Union entities on 30 October 2024.

Priorities, challenges and opportunities for 2025

Digital transformation is a key driver of innovation and modernisation of the European public administration. At the same time, it creates new cybersecurity risks and challenges, mostly by increasing the attack surface and by introducing additional potential vulnerabilities, not least due to technological evolutions (e.g. cloud, quantum computing or artificial intelligence).

The **first important milestones** since the entry into force of the Regulation have been achieved, showing the determination of Union entities to take a **solid and common action** to improve their cybersecurity. At the same time, these achievements have permitted to further explore and **identify issues which require attention** going forward and which, if solved, would allow Union entities to be even more efficient.

The immediate priorities are **the implementation of the upcoming milestones**. This requires **closer interinstitutional cooperation**, under the lead of the IICB and thanks to the help and renewed mandate of CERT-EU, as well as **specific actions,** including more harmonisation and standardisation. In parallel, it will be important to promote **Union-level cooperation**, including by deepening engagement with the Member States and the private sector.

Providing Union entities with **adequate support, including resources, and up-to-date tools** for reinforcing their resilience and protecting their cybersecurity will contribute to **ensuring a safer and more secure Europe, better equipped to protect our democracy and to uphold our values.**[15]

"World peace cannot be safeguarded without the making of creative efforts proportionate to the dangers which threaten it".[16]

In addition, going forward, **five points deserve particular attention**:

1. Investment in cybersecurity.
2. The role of the IICB.
3. New ways of working among Union entities.
4. New ways of working with third parties.
5. Human resources for cybersecurity.

These points represent the challenges and the opportunities with a high impact on the perspectives of ensuring further reinforcement of cybersecurity at Union entities. They will be the object of discussions, recommendations and decisions for which the IICB will seek **guidance, agreement and support at the political level**.

1. Investment in cybersecurity

The Regulation responds to the geopolitical landscape, also taking into account the European Court of Auditors special report on cybersecurity of EU institutions, bodies and agencies,[17] which noted **a level of preparedness** overall not commensurate with the threats. The recent Niinistö report confirms and reinforces the need for higher preparedness, acknowledging a widening **threat landscape along with**

[15] In reference to: Europe's Choice - Political Guidelines for the Next European Commission 2024-2029.
[16] Schuman Declaration, Schuman declaration May 1950 | European Union (europa.eu).
[17] Special report 05/2022: Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats | European Court of Auditors.

the cyberattack surface, leading to bigger possible repercussions for the Union**. But regulation** alone is not enough. **Investment** in cybersecurity is just as important, so as to equip the Union entities with **adequate means** to shield themselves from these threats. Indeed, the Regulation already highlights that Union entities should aim to allocate a percentage of their ICT budget to improve cybersecurity, and that in the longer term an indicative target of at least 10 % should be pursued.

At the same time, the lessons learnt and achievements from the first year of implementation of the Regulation highlighted the need to **focus not just on the level of the investment, but on where it should be directed**. Indeed, the target of 10% may **apply to Union entities differently**, as maturity levels are not the same. In this regard, the **maturity assessment** to be performed by all Union entities by 8 July 2025 is particularly important. The exercise will allow to further refine and justify **where the investments are needed to have the highest positive impact**, to prioritise and focus on the most urgent and efficient solutions, and to plan the best course of action.

The findings will provide a **valuable contribution to budgetary discussions**. In the more immediate term, this would occur within the context of the annual budgetary review. In the longer term, and in line with the priorities and aspirations for the next 5 years,[18] a **simpler, more focused and responsive Multiannual Financial Framework** that is **fit for purpose and reflects European strategic priorities and ambitions** should **embed the growing importance of cybersecurity** to unlock the funding.

2. Role of the IICB

The IICB is an **important forum to communicate and promote cybersecurity and resilience**. In this regard, the experience of facilitating the cooperation among the Union entities places the **IICB as a valuable source of inspiration** for other stakeholders in the field, with a **positive influence** going beyond the EU inter-institutional context.

For instance, by exchanging expertise, promoting common cybersecurity standards and ways of working, or common services, the work of the IICB can **inspire the working methods across the EU public administration**. Some of the challenges experienced by the Union entities may be similar to those faced by the organisations in the **Member States**, including in the **private sector**, when implementing national or EU legislation. By sharing the lessons learnt and promoting best practices, the IICB would not only strengthen the inter-institutional cooperation but also help build mutual trust, minimise risk exposure, and further improve the security culture across EU.

Similarly, the IICB should be able to participate in relevant forums and **welcome** ideas on common challenges and practices, which could lead to new reflections. The IICB should therefore **proactively engage** at different levels. In this respect, **structured communication** with other bodies in the EU public administration, such as the relevant Working Group(s) in the Council or European Parliament's Committee(s), as well as organisations across the EU and outside, including by leveraging the experience of ENISA, should be promoted.

Increasing the strategic visibility of its actions would additionally benefit the **European democracy**, by allowing citizens and stakeholders subject to similar cybersecurity rules to witness the EU public administration's **entrepreneurship and willingness to lead by example** in the areas where it legislates.

Last but not least, by being more assertive in establishing high levels of cybersecurity, the IICB would contribute to the EU's **resilience and strengthen its deterrence by denial**, sending a clear signal to

[18] In reference to: Europe's Choice - Political Guidelines for the Next European Commission 2024-2029.

threat actors on its determination to develop the capabilities to prevent, protect, respond and recover from cyberattacks.

3. New ways of working among Union entities

Union entities would greatly benefit from **adopting and embracing new ways of working**. Notably, this would enhance cooperation, including in the forms of sharing capabilities and knowledge, potentially leading to economies of scale. Once more, coupled with a purposeful increase of resources, this would reinforce the **effectiveness of allocation, which would be directed exactly where needed**.

Such collaboration would require **high discipline, strong commitment, and a shared approach towards the implementation of cybersecurity best practices** to avoid a single point of failure. However, and most importantly, it would enable Union entities to **safeguard even more their institutional autonomy** against rising internal and external threats, thanks to a common posture and combined efforts towards the same goal. This perfectly aligns with the purpose of the legal basis on which the Regulation is built:

> *"In carrying out their missions, the institutions, bodies, offices and agencies of the Union shall have the support of an open, efficient and independent European administration".*[19]

In 2024, the IICB and its Executive Committee advanced several ideas on how interinstitutional collaboration could be adapted to the new needs stemming from increased digitalisation, and to avoid duplication of the same tasks across different Union entities. Examples include **combined service offerings** under the lead of CERT-EU, **harmonisation of cybersecurity requirements**, **coordinated procurement** or **common cloud infrastructure**. In turn, this would have positive repercussions on **European tech sovereignty and competitiveness** as well, by making it more sustainable and better equipped to act more independently in a globalised environment.

4. New ways of working with third parties

As mentioned in the introduction, **supply chain attacks** have been particularly challenging in 2024. When it comes to Union entities and their vicinity, threat actors often breached them by exploiting the vulnerabilities in the internet facing software products. As of early November, CERT-EU estimated that 90 software products from about 50 vendors, used or highly likely used by Union entities, have been targeted since the beginning of 2024. The existence of so many products lacking basic security standards, with flawed development or maintenance processes, delays in reaction time for patching from some vendors, and difficulty in collaborating, is **alarming**.

While Union entities can only react through soft measures, like stronger procurement rules and screening, this problem possibly calls for a wider policy solution.

The **Cyber Resilience Act** is a first important step in this direction, as it introduces mandatory cybersecurity requirements for manufacturers and retailers of products or software with a digital component.[20]

At the same time, the above proves the importance to **monitor the security posture of Union entities in relation to their suppliers**. An example could be to adopt common guidelines for the use of service providers, and to ensure that the security baseline rules for remote service delivery remain updated.

[19] Treaty on the Functioning of the European Union, Article 298. EUR-Lex - 12016E298 - EN - EUR-Lex.
[20] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

This would enhance the protection of ICT systems and information against the risks arising from outsourcing, especially due to increased complexity and new cybersecurity threats.

Another way to address this issue would be **CERT-EU's Full-Spectrum Adversary Approach**, mentioned earlier. Indeed, by analysing threats to Union entities in all their dimensions, mitigation and detection measures related to supply chain security could be applied in a more comprehensive way.

Finally, the **experience** of Union entities in dealing with third-party security should be shared, to draw lessons learnt, anticipate challenges, and ensure preparedness on common threats.

5. Human resources for cybersecurity

Building and developing adequate capabilities is a **vital** imperative that relies on Union entities' capacity to **attract and retain talent in a scarce job market**. The demand for experts in cybersecurity is skyrocketing, outpacing the rate at which talent enters the market. Union entities additionally compete with the private sector for a **limited pool** of qualified candidates, making the recruitment process more challenging. **The IICB has stressed several times that insufficient staffing and limited access to continuous competence development opportunities** for qualified expert staff is a **major challenge** that needs to be addressed. This affects **all Union entities**, and particularly the smaller ones, especially in light of the new obligations stemming from the Regulation.

In November 2022, the European Parliament, the Council and the Commission, in the context of the negotiations on the Budget 2023, issued a joint statement on cybersecurity, recognising the necessity of adequate capacity to respond to cybersecurity threats and incidents. The announcement was followed by a report, drawn up in 2023 by the Commission in close cooperation with CERT-EU and the other institutions, to provide an overview of current cybersecurity staffing across institutions, and an assessment of the needs. According to this report,[21] **Heading 7 institutions and bodies indicated 177 Full Time Equivalents of additional cybersecurity staffing needs for the period 2023 - 2027**. This figure comes **on top of the resource needs for CERT-EU** following the entry into force of the Regulation, and of Union entities not covered under Heading 7.

Fully acknowledging the **necessity for long-term solutions**, the IICB recognised the **urgency** to identify and apply **intermediate measures** to mitigate the exposure of Union entities to the negative consequences of resource and competence gaps. In this respect, **cooperation, synergy and solidarity** are crucial. This is, indeed, the "spirit" conveyed through the IICB's Multiannual Strategy, and the will of the Union entities to engage on this path is demonstrated by the creation of the **LCO Network,** the **TAGs,** the **concept of combined service offerings**, and the contribution provided via the **Full Cooperation Mode.**

Notwithstanding the above, a budget which is **more focused on further reinforcing cybersecurity is a strategic priority** and a **matter of political credibility** for the years to come. Indeed, it would confirm the **determination** to invest in the development of cybersecurity capabilities, as a **commitment** to the goals announced at the **political level**. This is crucial for **staying on course** and maintaining the high pace of progress required to **remain ahead of the fast-evolving threats**, at a time of increasing geopolitical tensions and strategic rivalries, as well as the growing use of emerging technologies for offensive purposes.

[21] Overview of current cybersecurity staffing across Heading 7 institutions and assessment of the needs.

Overall assessment and conclusions

Cybersecurity remains a **challenge**, but more importantly, a **significant opportunity** to boost European security, democracy, preparedness, resilience and credibility. In light of the threat landscape and reflections from the work of the IICB, this report, and the Niinistö report, it is clear that **Europe needs to be more assertive** and build further its deterrence power. **Union entities must be equipped** with the right tools and resources to do so, and **act jointly and unitedly** to face the current and future multifaceted threats with the crucial help of CERT-EU.

The entry into force of the Regulation in January 2024 marked the beginning of a journey, **engaging the highest level of management** and the cybersecurity community of all Union entities in a joint endeavour, with the support of the IICB, towards an ambitious goal. Along this path, aware of the challenges and expectations, the IICB swiftly completed its setup, adopted a **Multiannual Strategy**, approved the **essential guidelines** within the specified deadlines, and took several decisions to **stimulate cooperation** among Union entities with the help of **CERT-EU**. The **members of the IICB** undertook their new responsibilities, **demonstrating their genuine commitment** to act and work together in this forum, on top of the day-to-day duties in their respective organisations, reflecting a mindset of **accountability and leadership**.

CERT-EU had to review and adjust its organisation to match the new mandate, which it did successfully under the renewed leadership. In full transformation mode, CERT-EU managed to assure and sustain a **high-pace and quality** in developing and disseminating the guidelines and in creating and reinforcing the means of cooperation and support for Union entities. At the same time, CERT-EU kept delivering the services in all the areas covered by its service catalogue, while challenged by the sustained occurrence of significant cybersecurity incidents.

Aware of their obligations, and sensitive to the importance of cooperation, the **Union entities invested their time in planning the necessary actions**, encouraged their experts to join the newly established cooperation structures, interacted with CERT-EU signalling the needs for additional support, and shared the identified challenges with the IICB.

This first year of activity has been concluded successfully, setting a solid ground for the next steps – structurally, strategically and operationally. The results of 2024 will serve as the **basis for the actions** foreseen in 2025. The IICB will steer and monitor the progress. This will form the basis of an **assessment** that will allow to **detect further challenges and identify the opportunities** emerging from this experience. This assessment may lead to specific recommendations that the IICB may produce pursuant to Article 25 of the Regulation.

However, **the above is only the beginning of the journey**. As Union entities start the second year of the implementation of the Regulation, the progress achieved in 2024 should **encourage and inspire continued efforts** to maintain the momentum and focus. This will require **readiness and political determination to evolve and invest**, providing the necessary means to turn priorities into results, as it will **affect the ways of working** of the EU public administration. At the same time, it will be **crucial to ensure the EU's resilience** in the face of growing threats, and to adapt to change where such change is needed to **protect and uphold** the Union's (cyber)security, autonomy, democracy, and way of life.

Annex I - Achievements and progress with the implementation of the Regulation in 2024

1. Overview of timeline of the IICB's work

Article 10(8) of the Regulation states that "*The IICB shall meet at least three times a year at the initiative of its Chair, at the request of CERT-EU or at the request of any of its members*". In 2024, the IICB held its ordinary meetings on 23 February, 24 June and 29 November 2024. Furthermore, to respect the deadline on the approval of guidelines pursuant to Article 5(1), an extraordinary meeting was held on 6 September 2024. Nevertheless, the IICB continued to work throughout the year and in-between meetings, to prioritise its tasks based on the needs of Union entities related to the implementation of the Regulation.

The Executive Committee of the IICB, promptly established during the meeting of 24 June 2024, met three times: on 11 July, 29 August and 25 October 2024, to address the tasks entrusted to it by the IICB.

2. Notable decisions adopted by the IICB

Below are some of the main Decisions which allowed the IICB to either start functioning as swiftly and efficiently as possible, or to meet the obligations of the Regulation and help Union entities fulfil their tasks.

- IICB24D002 on the approval of the Rules of Procedure of the IICB.
- IICB24D005 on approving guidelines on arrangement, format and content of reporting of significant incidents.
- IICB24D007 on the appointment of the Head of CERT-EU.
- IICB24D009 on the appointment of the Chair and Deputy Chair of the IICB.
- IICB24D012 on approving the IICB Multiannual Strategy for 2024 - 2029.
- IICB24D013 on approving guidelines on the framework, maturity assessment, risk management measures and cybersecurity plan.
- IICB24D014 on approving guidelines on incident response coordination and cooperation for significant and major incidents.

3. Implementation of the Multiannual Strategy

a. Strategic Objective 1 – Fostering cooperation of Union entities on the full cybersecurity spectrum

Reporting on Technical Advisory Groups

The **Technical Advisory Group on CERT-EU guidelines proposals** was created with the objective to review the guidelines drafted and proposed by CERT-EU pursuant to Article 5(1) of the Regulation. The goal was to suggest pragmatic, effective, and cost-effective improvements of these guidelines, after reaching a consensus in the TAG. After its kick-off meeting on 14 May, the TAG met 6 more times until June and delivered its document with consolidated comments to CERT-EU by 18 June. Following the approval of the guidelines, this TAG has been put on hold.

The **Technical Advisory Group on Tools and Methodologies** consists of cybersecurity experts with a diverse skill set engaged in developing and operating information on cybersecurity tools and methodologies to help the IICB, CERT-EU and Union entities in applying appropriate cybersecurity risk management measures. Following a gradual transition from the informal ICDT CSSG Task Force on Services (which organised presentations for the community on tools and best practices), the TAG was formally established by the IICB in July 2024. The TAG had its online kick-off meeting on 26 September, which was well attended, and where the Work Programme, which included the deliverables, and the logistics of the group were presented and discussed. The Work Programme goes into several priority areas and subdivides the year into various phases, with the objective of the TAG being to engage in studying and analysing the most pressing Tools and Methodology challenges facing Union entities. To this end, the first phase of the TAG's work programme, which ended in late November, produced three outputs: validating the ENISA Risk Assessment Methodology, creating a list of AI tools and usage to defend against major threats, and mapping the Essential Eight[22] to other maturity models.

The **Technical Advisory Group on the Human Factor** was established by an IICB Decision in June 2024. The TAG deals with Cybersecurity Training and Awareness raising, with the goal to strengthen a common cybersecurity culture across the board for all Union entities. As such, it builds on and continues the work of the former ICDT CSSG, particularly Task Force 4 on Cybersecurity Training, and Task Force 5 on Cybersecurity Awareness Raising. Such continuity is also provided by the TAG Chair, who is from the Commission and also chaired Task Force 5. Key members of both Task Forces are present in the TAG, ensuring knowledge transfer and continuity of activities. The TAG includes a working group dedicated to skills and cybersecurity training, led by ENISA.

The first meeting of the TAG took place on 6 September and focused on brainstorming on its priorities and activities. The first joint activity was the organisation of the interinstitutional kick-off meeting for the European Cybersecurity Month (ECSM) on 2, 3 and 4 October 2024. It was also a first occasion for TAG members to meet and share best practices, experience and resources. The second meeting, on 30 September, focused on sharing information and experience related to the organisation of ECSM activities. Other activities of the TAG include the organisation of an interinstitutional phishing exercise and the sharing of resources. The third European cybersecurity skills conference in Budapest (26-27 September) provided a solid basis on which to build activities for the TAG.

b. Strategic Objective 2 – Providing strategic direction to CERT-EU and accompanying its development

Appointment of the Head of CERT-EU and other notable Decisions

Article 15(1) of the Regulation states that "*the Commission, after obtaining the approval of a majority of two thirds of the members of the IICB, shall appoint the Head of CERT-EU".* Such appointment was crucial to ensure continuity of work of CERT-EU, particularly important during the first year of application of the Regulation and the duty of CERT-EU to propose guidelines to the IICB. Within this context, following the selection procedure in the European Commission, the IICB approved the appointment of the Head of CERT-EU in May 2024.

[22] The Essential Eight are mitigation strategies designed to protect organisations' internet-connected information technology networks developed by the Australian Signals Directorate, a member of Australia's national security community. For more information, see: Essential Eight Explained | Cyber.gov.au and About | Australian Signals Directorate (asd.gov.au).

Definition of reporting and interaction mechanisms between Union entities and CERT-EU

In alignment with its tasks, CERT-EU actively collects significant incident reports, and provides statistical data to the IICB on at least a quarterly basis.

Furthermore, during the IICB meeting on 6 September, regarding communication on the implementation of the guidelines, and particularly on the cybersecurity plans and reviews, the Chair indicated that documents would be requested from Union entities by the IICB, and that CERT-EU would be tasked to analyse them and report to the IICB.

Setup of organisational measures and communication channels to ensure the streamlining of information

To ensure efficient and streamlined communication on the various aspects of the implementation of the Regulation, the following channels have been established or, where they already existed, confirmed:

- The Secretariat of the IICB communicates to IICB Members and Alternates *via* a Functional Mailbox. In turn, the IICB representatives communicate to their Union entities. The Secretariat set up a secure online repository where the documentation related to IICB meetings and deliberations is stored and to which IICB Members, their Alternates, and Executive Committee Members have access.
- Further information distribution is performed by CERT-EU to the LCOs of all Union entities through the LCO Network with the support of ENISA. This informal Network aims to foster collaboration, knowledge-sharing and mutual assistance. The establishment of this Network was substantially supported by CERT-EU *via* the definition of rules and the setup of a dedicated channel on CERT-EU's exchange platform. The Network was officially launched in its inaugural plenary workshop on 22 November 2024.
- The EUAN representatives in the IICB are responsible, pursuant to Article 10(12) of the Regulation, for relaying the IICB's decisions to the members of the EUAN. In turn, EUAN members should raise with those representatives or the Chair of the IICB matters they consider should be brought to the IICB's attention. Discussions on the implementation of the Regulation also take place within the EUAN's Information and Communication Technologies Advisory Committee (ICTAC). Within this context, the Secretariat of the IICB was invited to ICTAC meetings on two occasions (25 April and 13 September) to provide status updates.

4. Overview of upcoming deadlines for the Union entities

In line with the obligations under the Regulation, Union entities and the IICB will need to meet the following deadlines for 2025:

- **8 April 2025**: "*each Union entity shall, after carrying out an initial cybersecurity review, such as an audit, establish an internal cybersecurity risk-management, governance and control framework (the 'Framework'). The establishment of the Framework shall be overseen by and under the responsibility of the Union entity's highest level of management"* (Article 6(1)).
- **8 July 2025**: "*each Union entity shall carry out a cybersecurity maturity assessment incorporating all the elements of its ICT environment"* (Article 7(1)).
- **8 September 2025**: "*each Union entity shall, under the oversight of its highest level of management, take appropriate and proportionate technical, operational and organisational measures to manage the cybersecurity risks identified under the Framework, and to prevent or minimise the impact of incidents"* (Article 8(1)).

- **8 January 2026**: "*each Union entity shall approve a cybersecurity plan*" (Article 9(1)).

In addition, in line with the guidelines adopted by the IICB pursuant to Article 5(1) of the Regulation, and to help prepare the different milestones, Union entities should approve an initial cybersecurity plan which, together with the initial review, would help constitute the framework. Similarly, a risk assessment should be performed together with the maturity assessment.

Annex II – Acronyms

IICB: Interinstitutional Cybersecurity Board

CERT-EU: Cybersecurity Service for the institutions, bodies, offices and agencies of the Union

Union entities: institutions, bodies, offices and agencies of the Union

ENISA: European Union Agency for Cybersecurity

EUAN: European Union Agencies Network

ICTAC: Information and Communication Technologies Advisory Committee

TAG: Technical Advisory Group

LCO: Local Cybersecurity Officer

FSAA: Full-Spectrum Adversary Approach

ICDT CSSG: Interinstitutional Committee for Digital Transformation - Cybersecurity Subgroup

ICT: information and communication technology

SLA: Service Level Agreement

ECSM: European Cybersecurity Month