STUDY

A UN Effect? How the EU Implements the Norms of Responsible State Behavior in Cyberspace

Dr Patryk Pawlak and Christina Rupp

July 15, 2026

Tech analysis and policy ideas for Europe

interface

Table of Contents

Executive Summary

In 2015, the international community successfully endorsed a catalog of eleven voluntary norms to guide responsible state behavior in cyberspace. Yet, these behavioral expectations of how states should and should not behave in the cyber domain, such as responding to requests for assistance and refraining from intentionally damaging critical infrastructure, do not shape international security through agreement alone. Their ability to enhance international stability and strengthen the resilience of the digital infrastructure on which societies depend on rests predominantly on whether and how governments translate them into laws, institutions, operational procedures, and patterns of cooperation. Over the past decade, UN Member States have made varying levels of progress in this regard, and the shift from commitment on paper to implementation in practice remains challenging.

To address these gaps and accelerate the norms' practical implementation, regional organizations are increasingly developing their own implementation approaches and support mechanisms. ASEAN published a norms implementation checklist last year, the European Union adopted a contribution on its implementation of the UN cyber norms for the upcoming first plenary session of the UN Global Mechanism on ICT Security next week, and the African Union is also in the process of developing implementation guidelines.

Against this backdrop, there is a need to better understand how states embed the specific responsibilities and expectations of restraint encapsulated in these norms into everyday governance. Given the emergence of a comprehensive cybersecurity policy ecosystem and complex institutional architecture, particularly in the decade since the UN cyber norms were formally institutionalized, the European Union provides a valuable case study for examining these dynamics.

Its experience offers insights into how states and regional actors align, adopt, and adapt their practices through two pathways: explicit and implicit **internal implementation** via legislation, policies, institutions, and partnerships; and **external implementation** via cyber capacity-building initiatives supporting norms implementation in partner countries and regions.

Specifically, analyzing the EU's implementation experience across these pathways yields several key takeaways:

- 55 identified internal implementation activities and additional external implementation examples across eight capacity areas demonstrate that the **EU is already implementing the UN cyber norms extensively and at scale** across its policy ecosystem. These measures are not confined to a single policy area or institution but are embedded across multiple governance domains.

- **The EU's norms implementation is an inherently dynamic and continuous process.** The EU experience demonstrates that implementing the UN cyber norms is not a single downstream step, but a prolonged process of translation, institutionalization, and revision.
- The **EU's implementation is driven by a set of cross-cutting enabling capabilities rather than isolated measures linked to individual norms**. These include cybersecurity coordination structures and agencies as well as regulatory regimes for critical infrastructure protection and cooperation in addressing cybercrime.
- **The EU's implementation appears most robust where political commitments are reflected in legislative frameworks with built-in enforcement mechanisms**, for example, by defining duties, creating compliance expectations, and empowering oversight actors.
- **The EU framework has translated positive commitments into regional practice more readily than prohibitive norms.** EU-level implementation efforts are strongest where behavioral expectations can be embedded in existing resilience, preparedness, and capacity building frameworks.
- **Critical infrastructure protection is one of the areas where EU measures aligning with the behavioral expectations reflected in the UN cyber norms are strongest.** This suggests that norms implementation can advance more quickly when it is tied to concrete public-interest functions.
- **The EU largely implements the UN cyber norms implicitly**. Many EU measures align substantively with the UN cyber norms, but they are rarely framed as contributions to the UN framework for responsible state behavior in cyberspace.

While the EU likely has one of the most mature norms implementation frameworks worldwide, many of its implementation building blocks – from cybersecurity coordination structures to regulatory frameworks addressing critical infrastructure protection – are also reflected in other implementation-focused initiatives. This points to growing cross-regional convergence around the practical foundations needed to operationalize the framework.

Even though the EU is in many ways unique in its approach to the implementation of the UN cyber norms, its experience can thus also offer insights for other regions and states interested in strengthening implementation. They include the added value of mapping norms also against institutional responsibilities, not only against laws and policies, building in revision pathways to help keep implementation adaptive, balancing common objectives and domestic execution at the regional level, and considering critical infrastructure protection as a particularly feasible and politically actionable starting point for broader norm operationalization.

These findings and reflections point to five recommendations for future EU engagement to accelerate implementation at both the internal and international levels:

1. The **EU should strengthen internal socialization of the UN cyber norms across its institutions, bodies, and agencies** to ensure a whole-of-EU perspective, so that the norms become part of everyday policymaking, not only diplomatic messaging.
2. The **EU should systematically track implementation internally across EU institutions and instruments** in order to identify existing practices, spot gaps, clarify responsibilities, and encourage Member State engagement, for example, through an annual internal "UN norms in EU practice" briefing.

3. Building upon its July contribution, the **EU should continue to move from implicit implementation to more explicit implementation narratives in public communication and international fora** that connect EU instruments and practices to the UN framework. This would serve multiple EU objectives at once, as it reinforces the practical relevance of the UN framework, showcases the EU's cybersecurity acquis, and supports implementation debates in other regions.
4. The **EU should embed a stronger implementation lens into its cyber capacity building efforts**, especially recognizing that many of its existing initiatives already support norm implementation, even though they are currently mostly not framed in those terms.
5. Finally, the **EU should leverage the UN Global Mechanism to advance the debate on implementation**, including through working papers, side events, and technical briefings, and by feeding insights from its implementation experience into any renewed work on a voluntary implementation checklist. In parallel, the **EU should deepen cross-regional engagement with implementation initiatives developed by other regional organizations**, particularly ASEAN and the African Union, to identify convergence on implementation activities, shared implementation challenges, and emerging good practices. The norms relating to critical infrastructure protection provide the most feasible and politically actionable entry points for broader cross-regional norm operationalization and mobilization.

As the new UN Global Mechanism begins its substantive work this year with a mandate to accelerate implementation, this mapping of the EU's norms implementation provides cyber diplomats with an evidence base for a more operational understanding of implementation in practice. It can also support them in designing targeted capacity building on implementation of the framework and identifying interlinkages of norms implementation practices across the cyber diplomacy toolkit, particularly with confidence-building measures and international law. Policymakers can use these insights to inform discussions in Global Mechanism working groups and cross-regional dialogues. This is particularly important at a time when the effectiveness of the UN cyber framework increasingly depends less on negotiating new commitments than on embedding existing ones into regional and national practice.

Introduction

Over the past twenty years, states have gradually constructed a framework for responsible state behavior in cyberspace through successive UN working groups, including Groups of Governmental Experts (GGEs) and Open-ended Working Groups (OEWGs).[1] This framework rests on several core pillars: States have affirmed that international law applies to cyberspace, agreed on 11 voluntary, non-binding norms of responsible state behavior, developed confidence-building measures (CBMs), advanced principles for cyber capacity building, and identified existing and emerging threats to international peace and security stemming from the use of information and communication technologies.

1 For a brief history of UN cybersecurity governance, see How cybersecurity became a UN issue, in: Christina Rupp (2026): The UN's New Global Mechanism on Cybersecurity: How Europe Can Advance Responsible State Behaviour in Cyberspace, interface.

Among these five pillars, the eleven norms adopted in the 2015 UN GGE report (see Figure 1) play an important role.[2] These norms provide political guidance for responsible state conduct in cyberspace by including both positive obligations ("do's") – such as cooperating to protect critical infrastructure and responding to requests for assistance – and prohibitive commitments ("don'ts"), including the expectation that states should refrain from intentionally damaging critical infrastructure or targeting Computer Emergency Response Teams (CERTs).[3]

2 United Nations General Assembly (2015): Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). The focus on norms implementation has grown significantly since the importance of norms and principles was recognized for the first time in the 2010 GGE report, which acknowledged the existence of norms relevant to using ICTs by States and the possible need to develop additional norms, United Nations General Assembly (2010): Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201). Although not formulated in the exact same way as today, norms of responsible state behavior and the need to implement them were already embedded in the 2013 GGE report, including the role that may be played by private sector and civil society organizations, United Nations General Assembly (2013): Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98).

3 The 2015 GGE report articulated their purpose as follows: "Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development," United Nations General Assembly (2015): Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174).

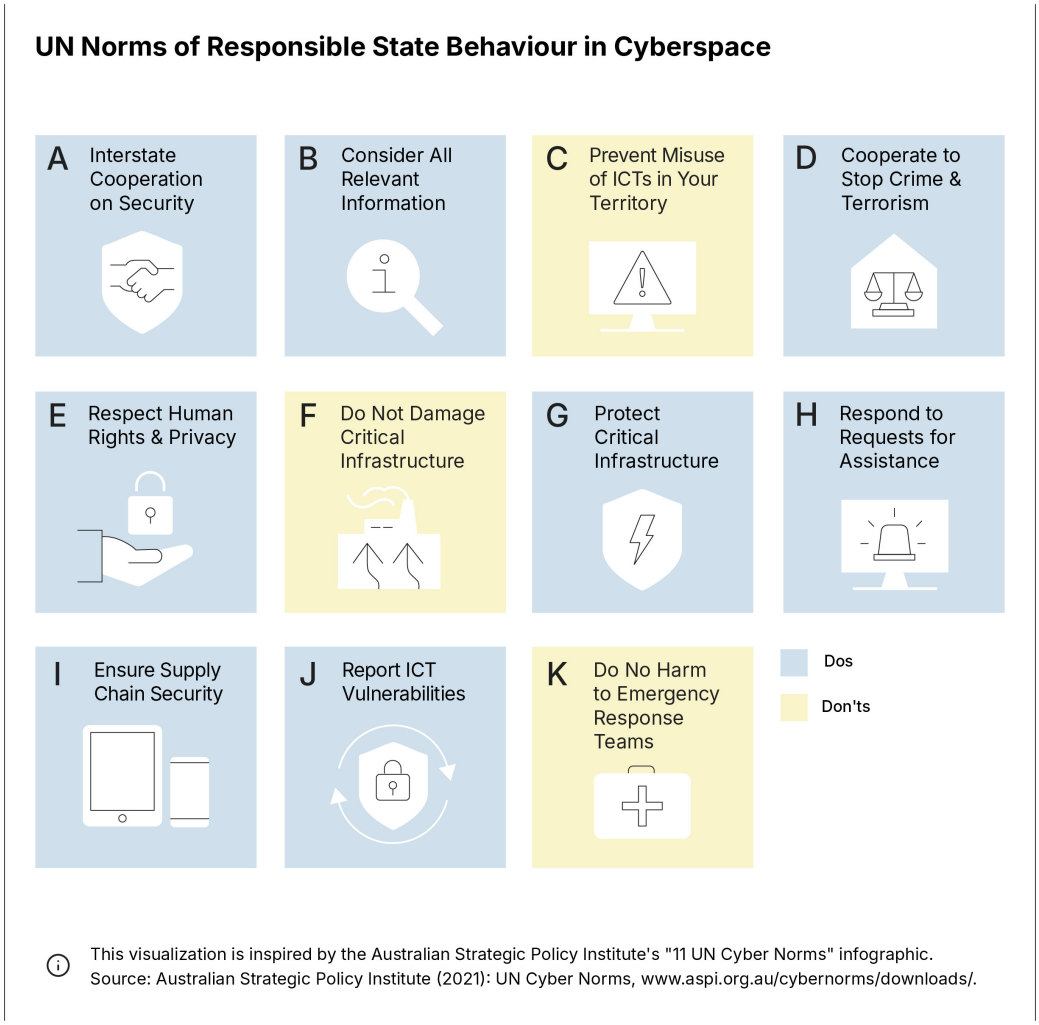

Figure 1: UN norms of responsible state behavior in cyberspace

The behavioral expectations contained in the norms matter not because they are automatically obeyed, but because they shape the kind of digital societies and international order states choose to build. Whether and how governments translate these commitments into laws, institutions, operational procedures, and patterns of cooperation can not only enhance international stability by increasing the predictability of state conduct. It also affects the security of hospitals, energy systems, public administrations, financial networks, and the wider digital infrastructure on which contemporary societies depend.

In that sense, implementing the UN cyber norms[4] is not a narrow technical discussion for diplomats or cybersecurity specialists. It shapes how international order is made concrete,

4 Throughout this paper, the authors use UN cyber norms in reference to the 11 norms of responsible state behavior agreed as agreed in the 2015 UN GGE and endorsed by subsequent GGE and OEWG reports.

how restraint and responsibility are embedded in everyday governance, and whose experiences and interests ultimately define what "responsible behavior" means in practice.[5] The repeated calls for additional guidance on implementation, including in the 2021 report of the UN GGE and the OEWG discussions, underscore that norms acquire meaning not only through diplomatic endorsement, but mostly through how they are operationalized in practice.

This raises a central question: To what extent do international cyber norms shape regional governance and state practice? And more specifically, does the UN framework generate what could be described as a "UN Effect"[6] by serving as a global reference point that influences how states approach cybersecurity governance in practice?

The European Union (EU) offers an important case study for better understanding these dynamics. Although the UN framework is directed at UN Member States, the EU plays a significant role in operationalizing international commitments. While EU Member States retain exclusive competence in foreign and security policy, where the framework for responsible state behavior is discussed, many cyber-relevant areas either fall under shared or exclusive EU competences or are strongly shaped at the EU level, particularly in the internal market, justice, and home affairs domains. Cybersecurity has also become embedded across other EU policy areas, where states collaborate and align their approaches. This has produced a comprehensive cybersecurity policy ecosystem and a complex institutional architecture at the EU level,[7] much of which has emerged in the decade since the UN norms were formally adopted.

This makes the EU both a useful and a complex implementation arena for studying how states align, adopt, and adapt practices in order to comply with and/or shape collective international behavioral expectations. It also demonstrates how regional organizations can contribute to putting the UN framework into practice, while also revealing the limits and diversity that can accompany implementation across multiple legal and institutional settings.

To unpack how the EU implements the UN cyber norms in its law and policy practice, this paper first delves into the conceptual underpinnings of norms implementation (Chapter 3.1), reviews the current state of norms implementation mapping efforts (Chapter 3.2), and discusses key challenges to norms implementation (Chapter 3.3). It then examines two pathways of implementation at the EU level: internal and external. The internal pathway analyzes how the EU implements each of the UN cyber norms

5 Louise Marie Hurel, Mariana Salazar Albornoz, Noran Fouad, Gavin Wilde, Patryk Pawlak and Gatra Priyandita (2025): Global Compendium on Responsible Cyber Behaviour, Royal United Services Institute for Defence and Security Studies.

6 By analogy to the "Brussels Effect," see Anu Bradford (2021): The European Union in a globalised world: the "Brussels effect," Revue Européenne du Droit 2.

7 interface (2025): EU Cybersecurity Policy Directory and Christina Rupp (2024): Navigating the EU Cybersecurity Policy Ecosystem: A Comprehensive Overview of Legislation, Policies and Actors, interface.

through EU-level legislation, policies, and institutional mechanisms (Chapter 4). The external pathway investigates how the EU supports the implementation of UN cyber norms in other parts of the world through cyber capacity building projects and initiatives (Chapter 5).[8]

In assessing these pathways, the paper adopts a broad understanding of implementation. Rather than limiting implementation to explicit regional declarations, dedicated implementation strategies, or direct references to the UN framework, it also examines implicit EU-level implementation through regulatory frameworks, institutional arrangements, operational procedures, and capacity building initiatives. What matters for this analysis is not whether a given EU measure was adopted in the name of a specific UN norm, but how closely the measures adopted at the EU level align with that norm's aims. This approach makes it possible to capture the ways in which regional governance can give practical effect to international commitments even where the connection remains indirect. This paper does not examine implementation activities at the EU Member State-level, including national legislation or activities falling within national prerogatives. This limit necessarily narrows the picture, but it also allows for a more rigorous assessment of what can presently be identified as EU-level contributions to norms implementation. The paper concludes with key takeaways for the EU (Chapter 6), reflecting on the insights that the EU's experience with implementing the UN cyber norms may offer outside the EU context (Chapter 7), and providing recommendations for future EU engagement to advance norms implementation (Chapter 8).

Given the complexity and rapid evolution of EU cybersecurity policy, this paper should be read as a living document rather than as an exhaustive mapping exercise. At a time when the implementation debate in UN cybersecurity governance gained renewed momentum through the establishment of the permanent UN Global Mechanism on ICT Security (UN GMech), the objective of this paper is not to provide a definitive assessment of the EU's compliance with the UN framework. Rather, it seeks to identify and assess existing implementation practices that contribute to the operationalization of the UN cyber norms, which can in turn feed into and inform intergovernmental deliberations. This matters because the effectiveness of the UN cyber framework increasingly depends less on negotiating new commitments than on embedding existing ones into regional and national practice and gaining a better understanding of how implementation takes place, including where it remains partial, uneven, or implicit.

8 Another analytical dimension could look at how the EU contributes to implementing the UN cyber norms through the so-called "Brussels effect" but this is outside the scope of this report.

From Norm Emergence to Norm Implementation

International relations scholars have long emphasized that norms evolve through processes of emergence, cascade, and internalization, and that practice, contestation, and social interaction shape their content.[9] Implementing the UN cyber norms is thus an inherently complex endeavor, as this process operates at the intersection of foreign and domestic policy. While states negotiate norms internationally, implementation depends on how they and regional organizations translate them into domestic and regional legislation, policies, institutional arrangements, operational procedures, and coordination mechanisms. To better understand what happens between norm emergence and norm implementation, the subsequent sections will delve into the conceptual underpinnings of norms implementation, review the status quo of norms implementation mapping efforts, and discuss key challenges to norms implementation.

Norms implementation as a process

The complexity surrounding the emergence and development of normative frameworks stems partly from the fact that implementation is not a one-way process in which states simply absorb internationally agreed norms at the domestic level. Rather, implementation and institutionalization unfold in parallel and mutually reinforce one another. This means that implementation can take place before, during, or after formal institutionalization, leading to different implementation trajectories across countries. It also means that not all states begin implementation from the same starting point and specific legal, political and societal circumstances will require local contextualization.

Broadly, this paper distinguishes three mechanisms (see Figure 2):

- **Alignment**, where states that contributed to shaping the norms effectively implement them by projecting their existing domestic practices onto the international level,
- **Adoption**, where states largely transpose the internationally agreed norms into domestic or regional frameworks with minimal modification, and
- **Adaptation**, where states tailor the norms to their specific legal, political, and institutional domestic contexts.

9 Martha Finnemore and Kathryn Sikkink (1998): International Norm Dynamics and Political Change, International Organization and Martha Finnemore and Duncan B. Hollis (2017): Constructing Norms for Global Cybersecurity, American Journal of International Law. Scholars have defined implementation as “a parallel process to institutionalization which draws attention to the steps necessary to introduce the new international norm’s precepts into formal legal and policy mechanisms within a state or organization in order to routinize compliance,” Alexander Betts and Phil Orchard (eds.) (2014): Implementation and World Politics: How International Norms Change Practice, Oxford University Press.

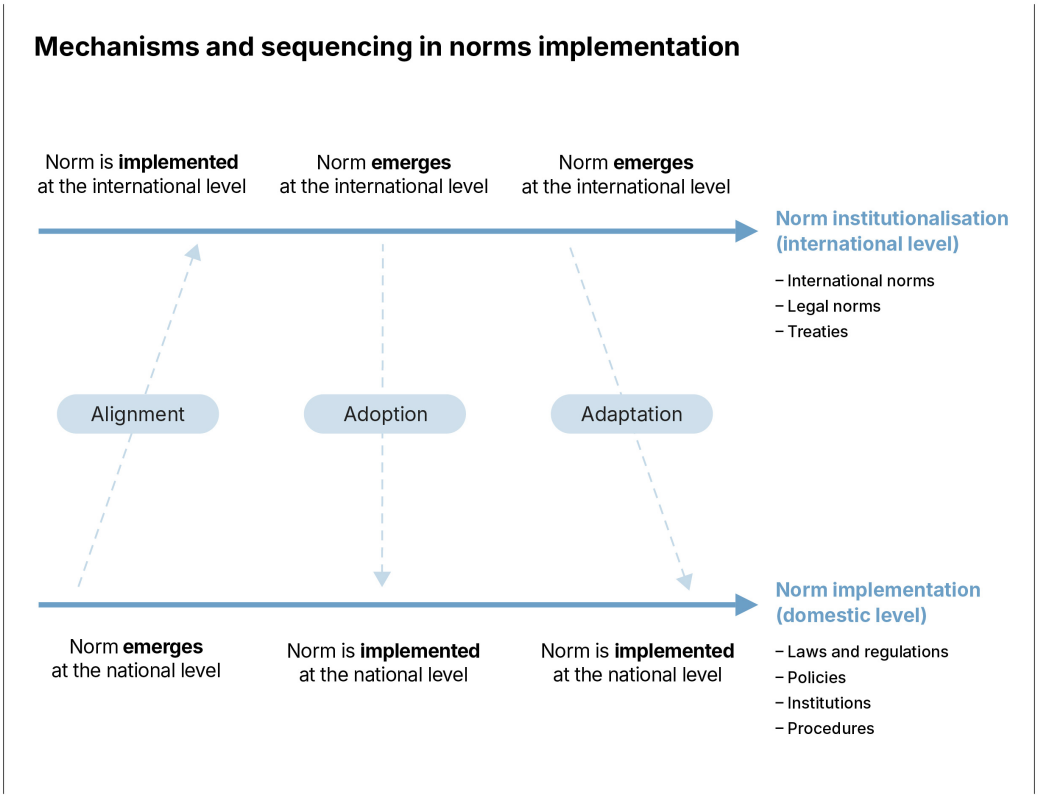

Figure 2: Mechanisms and sequencing in norms implementation

Differences in legal traditions, political priorities, institutional capacities, and administrative cultures may therefore result in divergent practices despite shared commitments. As the current international security environment shows, even when states subscribe to the same norms or incorporate them similarly into national legal systems, they do not necessarily implement those norms in the same way (adoption vs. adaptation).[10]

In this respect, mapping national and regional implementation experiences can help clarify ambiguities, expose contestation, identify capacity gaps, and generate practice from which more robust and legitimate international understandings can emerge. Implementation therefore represents both a means of operationalizing norms and a mechanism through which they continue to evolve.

State of play in mapping norms implementation

Despite the UN cyber norms having existed for more than a decade, only a limited number of states have publicly articulated systematic approaches to implementation.

10 Alexander Betts and Phil Orchard (eds.) (2014): Implementation and World Politics: How International Norms Change Practice, Oxford University Press.

Australia,[11] Canada,[12] Russia,[13] South Korea,[14] and the United Kingdom[15] – alongside a smaller cross-regional group of states advancing their interpretations of the due diligence norm (norm c)[16] – have published national position papers or implementation-oriented statements connecting domestic measures to specific norms. Within Europe, explicit implementation mapping remains limited. No EU Member State has yet published a comprehensive public mapping of how it implements the full catalog of UN norms. Czechia remains the only EU Member State – and also the only UN Member State overall – to have publicized its responses to the national implementation survey conducted by the United Nations Institute for Disarmament Research (UNIDIR).[17]

Even though there have been limited systematic national efforts to map norms implementation to date, the 2021-2025 UN OEWG has contributed to greater regional engagement on the issue, as regional organizations are increasingly adopting more implementation-focused approaches.[18] In the area of norms implementation, the Association of Southeast Asian Nations (ASEAN) has emerged as one of the most active regional actors through the development of a norms implementation checklist, accompanied by targeted capacity-building activities, which it adopted and published in February 2025.[19] Similarly, in 2026, the African Union has advanced its thinking on developing guidelines on norms implementation. In July 2026, the EU will present its contribution on its implementation of the 11 norms of responsible state behavior, connecting each to examples of the EU cybersecurity policy acquis.

Challenges to norms implementation

While states have succeeded in institutionalizing norms through negotiated consensus language, translating these commitments into practical policies, institutional structures,

11 Australian Department of Foreign Affairs and Trade (2020): Australian Implementation of Norms of Responsible State Behaviour in Cyberspace.

12 Government of Canada (2019): Canada's implementation of the 2015 GGE norms.

13 While Russia refers to a different catalog of norms, its publication of a norms implementation paper reaffirms the general importance of undertaking such a process, Russia (2021): Review of compliance of national legislation of the Russian Federation with the UN voluntary rules, norms and principles of responsible behavior of States in the field of international information security (Unofficial translation).

14 Republic of Korea (2020): Implementation of the 2015 UNGGE Norms.

15 United Kingdom Foreign & Commonwealth Office (2019): Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015.

16 Governments of Belgium, Czech Republic, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Portugal, Slovakia, and Spain (2024): Multiple States' views on best practices relating to the implementation of norm 13(c).

17 Czechia, in: United Nations Institute for Disarmament Research (n.d.): Cyber Policy Portal. The survey serves as a voluntary baseline assessment tool through which UN Member States can track their national implementation. It also asks states to identify challenges to implementation and/or specific gaps in capacity-limiting implementation, Helene Pleil (2025): The State of Cyber Confidence-Building Measures: How Governments Implement Multilateral Measures to Create Trust in the Cyber Domain, interface.

18 Other regional initiatives, including the African Union's common African position on the application of international law in cyberspace and the EU's common understanding on international law issued in 2024, likewise reflect a broader trend toward operationalizing the UN framework at the regional level (African Union (2024): Common African Position on the Application of International Law to the use of Information and Communications Technologies in Cyberspace and Council of the European Union (2024): Declaration on a Common Understanding of International Law in Cyberspace).

19 ASEAN (2025): ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace.

and operational procedures has proven far more difficult. Capacity gaps, persistent divergences, and growing geopolitical tensions have constrained implementation efforts. This became particularly visible during the final phase of the 2021-2025 UN OEWG, where states were unable to substantively advance a proposed voluntary checklist on norms implementation.[20]

At the same time, a broader political debate on implementation persists within the UN process. While many states increasingly emphasize the need to prioritize the implementation of existing commitments, others – including Russia, Iran, and Cuba – argue that implementation has become "overemphasized" and stress instead the need to continue developing new regulatory and legally binding instruments in parallel with technological change.[21] Other states, including EU Member States, have strongly opposed this position, maintaining that existing international law remains sufficient and that implementation should take precedence over negotiating additional commitments.

This divergence in views is also clearly recognized in the final report of the 2021-2025 OEWG, which notes that "the further development of norms, and the implementation of existing norms were not mutually exclusive but could take place in parallel."[22] Therefore, states reached consensus on the purpose of the new permanent mechanism by mandating the Global Mechanism, in the area of norms, to facilitate discussions on "voluntary, non-binding norms of responsible State behavior and the ways for their implementation, recognizing that additional norms could be developed over time."[23]

The implementation challenge is compounded by the nature of the norms themselves. Because the UN cyber norms are voluntary and only politically binding, implementation rarely follows a standardized or easily measurable pattern. Steps taken to put in place positive commitments,[24] such as building resilience or supporting cooperation, are generally easier to identify than prohibitive norms[25] that require restraint, non-use, or forbearance. Moreover, implementation is often implicit. States may operationalize elements of the UN framework through cybersecurity legislation, regulatory obligations, institutional mandates, incident response mechanisms, certification schemes, cybercrime

20 Chair Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (2025): Zero Draft - Final Report of the Open-ended Working group on security of and in the use of information and communications technologies 2021–2025, submitted to the 80th session of the General Assembly pursuant to General Assembly Resolution 75/240, Annex I.

21 United Nations General Assembly (2021): Open-ended working group on developments in the field of information and telecommunications in the context of international security - Final Substantive Report. See also Russian Federation et al. (2024): Updated Concept of the Convention of the UN on Ensuring International Information Security: Proposal of the Russian Federation.

22 United Nations General Assembly (2025): Developments in the field of information and telecommunications in the context of international security (A/80/257). The tension between consolidation and expansion also re-emerged during agenda-setting discussions at the Mechanism's first meeting in March 2026, the forum's organizational session, and ultimately led to the inability of states to agree on a plenary agenda. See further Christina Rupp (2026): From launch to delivery, the UN's new cybersecurity mechanism faces old divides, Binding Hook.

23 United Nations General Assembly (2024): Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (A/79/214).

24 Norms a, b, d, e, g, h, i, and j.

25 Norms c, f, and k.

cooperation, or capacity building initiatives without explicitly linking these measures to the UN norms themselves.

In this context, systematically mapping and documenting implementation practices becomes particularly important for the camp opposing the views of Russia and its like-minded partners. Demonstrating how states are already putting existing commitments into practice can help counter arguments that the current framework lacks practical relevance or cannot adequately address technological developments since the norms' adoption in 2015.

Internal Implementation: How the EU Implements the UN Cyber Norms

To analyze how the EU implements the UN cyber norms internally, this paper focuses on three main mechanisms of implementation: (1) legislation,[26] (2) policies,[27] and (3) institutions and partnerships. The paper covers legislation already in force as well as published policy documents, institutional arrangements, and other relevant initiatives, but does not include measures still under deliberation. Although this framework is applied specifically to the EU context, this approach also offers a useful framework for undertaking a norms implementation status quo analysis in other regions and countries.

Legislation

Legislation represents the most formal mechanism of norm implementation, translating broad international commitments into binding legal obligations on all actors operating within a given jurisdiction. In the EU, legal instruments vary in legal force and are often aimed at harmonizing or approximating laws in the EU's internal market. Key legislative instruments of the EU include Regulations and Directives. Regulations adopted by the EU are directly applicable and binding in full in all EU Member States. This means that even in cases where an EU Member State fails to enact national legislation reflecting the framework established at the EU level, entities and individuals operating in the territory of that state can still rely directly on the text of the EU act. Directives are binding as to objectives but require national transposition by each of the Member States. For Directives, implementation modalities are largely left to Member States, so that even when they set the same objectives, Member States retain flexibility in how to achieve

26 See further also European Union (n.d.): Types of legislation.

27 Legislation and policies frequently stipulate or embed standards and procedures, which translate norms into operational practices. Standards provide technical, legal, or professional guidance on acceptable behavior within the cyber ecosystem and support accountability across public and private actors. Procedures operationalize norms through internal and external processes, including whole-of-government coordination, cyber diplomacy, crisis management communication, attribution processes, and information-sharing mechanisms, thereby contributing consistent implementation across various administrative and operational contexts.

them. This can lead to differences across the EU in classification, institutional set-ups, and enforcement practices, which may sometimes trigger additional regulatory action.

Policies

Policies translate norms into political commitments, strategic priorities, and governance frameworks that guide implementation across institutions and Member States through soft law instruments. They are typically non-binding but politically authoritative. At the EU level, relevant policy instruments include cybersecurity strategies, Council conclusions, and Joint Communications from the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. These documents express political positions and set priorities without creating legal obligations. They do, however, create certain expectations among EU Member States regarding their intentions and conduct.

Institutions and Partnerships

Implementation requires structures and actors responsible for applying norms in practice. At the EU level, dedicated bodies such as the European External Action Service (EEAS) and the European Union Agency for Cybersecurity (ENISA) operate alongside numerous EU institutions integrating cybersecurity into sectoral mandates, meaning that some actors contribute to the implementation of UN cyber norms even though this is not explicitly provided for in their mandate. They are complemented by Member State cooperation structures such as the NIS Cooperation Group. Given their cross-cutting involvement across most of the implementation activities identified, the European Commission and individual Directorates are not specifically mentioned, as they have a stake in some form or another in the implementation of every norm. Beyond institutions, partnerships are essential for the operationalization of UN cyber norms because many imply cooperation with other states and stakeholder groups, for example, through bilateral and cross-regional dialogues, multistakeholder cooperation, and capacity building initiatives involving governments, the private sector, and technical communities.

For each of the eleven norms, the following sections are organized into four parts. They begin with the original wording of the norm, followed by a set of key questions for assessing relevant EU implementation practices.[28] Every section then summarizes the actions identified as supporting the norm's objectives before discussing each corresponding EU-level measure in greater detail. The identified activities deliberately span various fields and dimensions, including strategic, policy, operational, technical,

28 These questions are partly based on, and adapted from, the draft voluntary checklist of practical actions for the implementation of voluntary, non-binding norms of responsible State behavior in the use of ICTs.

legal, and diplomatic areas, all of which are relevant to norms implementation given their broad nature.[29]

The Annex provides a tabular overview of the identified EU implementation activities. The identified activities do not constitute a normative assessment of what (other) states should do in implementing the UN cyber norms.

Interstate cooperation on ICT security (Norm A)

Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

Key question(s) for assessing the EU's norm implementation:

- Q1: How does the EU cooperate with others in developing and applying measures to increase stability and security in the use of ICTs?
- Q2: How does the EU cooperate with others to prevent ICT practices that are acknowledged to be harmful, or that may pose threats to international peace and security?

Examples of activities that support the objective of enhancing interstate cooperation in the area of ICT security:

- Integrating international cooperation as a core pillar of cybersecurity strategies and other strategic or policy documents;
- Committing to and promoting the Framework for Responsible State Behavior in cyberspace;
- Establishing a national/regional framework for coordinated response to large-scale cyber incidents and crises;
- Developing a national/regional procedure for diplomatic responses to malicious cyber activities;
- Developing a national/regional posture in cyber defense;
- Articulating a national/regional position on the applicability of international law in the cyber context; and
- Engaging in bilateral, regional, and multilateral cooperation at technical, operational, and diplomatic levels.

The following sections provide an overview of the EU's approach to implementing these activities.

29 This approach is also reflected in the ASEAN Norms Implementation Checklist, ASEAN (2025): ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace.

— Integration of international cooperation as a core pillar of regional cybersecurity strategies and other strategic or policy documents and commitment to and promotion of the Framework for Responsible State Behavior in cyberspace

International cooperation is one of the key pillars of the EU's approach to secure its cyberspace and is reflected in many strategic and policy documents. The EU's latest Cybersecurity Strategy[30] adopted in 2020 clearly states that "international cooperation is essential to keeping cyberspace global, open, stable and secure." Consequently, the strategy emphasizes that the EU should "work with international partners to promote a political model and vision of cyberspace grounded in the rule of law, human rights, fundamental freedoms and democratic values that bring social, economic and political development globally." The EU Cybersecurity Strategy is also explicit about the need to advance responsible state behavior in cyberspace. In terms of concrete tools, the strategy proposes several regulatory and institutional solutions.

The EU's vision and approach to international cooperation have been further refined in the policy document defining the EU's Cyber Posture, adopted in 2022, which stresses the importance of "continued efforts to uphold and promote the UN Framework for responsible state behaviour" and underlines that "the EU and its Member States will actively work towards strengthening its implementation."

The EU's 2025 International Digital Strategy identifies the promotion of a high level of security for the EU and its partners as one of its three core objectives. In the field of cybersecurity, the strategy emphasizes that strengthening the cybersecurity and cyber defense capacities of partner countries would represent a direct investment in the EU's own security. In this respect, support for EU candidate countries is highlighted as a particular geographic priority. In terms of cooperative measures, the strategy, inter alia, envisages advancing cyber dialogues with partner countries, continued cybersecurity cooperation by the European Union Agency for Cybersecurity (ENISA) with third countries, and the implementation of cyber capacity building projects worldwide (see Chapter 5 for a more detailed discussion on how EU-level capacity building initiatives support the implementation of the UN cyber norms).

— Establishment of a regional framework for coordinated response to large-scale cyber incidents and crises

The guidance on the implementation of norm a by the 2019-2021 UN GGE highlights the establishment of crisis and incident management mechanisms as one of the means of

30 See also Council of the EU (2021): Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy.

putting the norm into practice. EU Member States retain the "primary responsibility for the response and remediation in case of a cybersecurity incident, a large-scale cybersecurity incident, or a cyber crisis affecting them."[31] Nonetheless, under the NIS2 Directive, EU Member States are required to designate a national competent authority "responsible for the management of large-scale cybersecurity incidents and crises," put in place a "national large-scale cybersecurity incident and crisis response plan,"[32] and "identify capabilities, assets and procedures that can be deployed in the case of a crisis."

These responsibilities are complemented by the relevant provisions of the NIS2 Directive and by the EU's Cyber Blueprint, which has provided a framework for coordinated responses to large-scale cyber incidents and crises, particularly those with cross-border implications, since 2017 and was updated by Member States in 2025.[33] The Cyber Blueprint is complementary to existing EU crisis management mechanisms at the EU level such as the integrated political crisis response (IPCR) arrangements. It sets out the modalities and responsibilities of actors at technical, operational, and political levels to clarify interactions among EU Member States' structures, coordination bodies, and EU institutions, bodies, and agencies across stages ranging from preparedness, detection, and response to public communication and lessons learned.

The European Cyber Crisis Liaison Organisation Network (EU-CyCLONE), formally established through the NIS2 Directive in 2023 (launched already in 2020), supports the coordinated management of large-scale cybersecurity incidents and crises within the European Union. EU-CyCLONe comprises the national cyber crisis management authorities designated by all EU Member States, with the European Commission participating in an observational capacity. Its tasks include "assess[ing] the consequences and impact of relevant large-scale cybersecurity incidents and crises and propos[ing] possible mitigation measures," as well as "support[ing] decision-making at political level in relation to such incidents and crises."

— Development of a regional procedure for diplomatic responses to malicious cyber activities

The Cyber Diplomacy Toolbox adopted by EU Member States in 2017 (with implementation guidelines revised in 2023) provides a detailed overview of tools and

31 Council of the EU (2025): Council Recommendation on an EU blueprint for cyber crisis management.

32 NIS2 requires the national plan to stipulate, in particular: "the objectives of national preparedness measures and activities; the tasks and responsibilities of the cyber crisis management authorities; the cyber crisis management procedures [...]; national preparedness measures, including exercises and training activities; the relevant public and private stakeholders and infrastructure involved; [and] national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level" (Art. 9(4) points (a)-(f)).

33 In 2024, ENISA also published a related report on best practices for cyber crisis management, ENISA (2024): Best Practices for Cyber Crisis Management.

instruments at the EU's disposal to jointly respond to and advance cooperation with third countries in cases of malicious cyber operations against the EU and its allies.[34] The toolbox, inter alia, includes preventive, cooperative, stability, and restrictive measures ranging from awareness raising on EU policies to coordinating political attribution of a cyber operation or campaign. The guidelines lay out a nine step-process for the development of a common EU position.[35] The 2023 guidelines further note the added value of further exploring strengthened cooperation with non-EU countries, private sector entities, and international organizations. Concerning EU-NATO cooperation, the 2023 guidelines stress "possible coordinated responses to malicious cyber activities [... and] seek[ing] potential synergies between the respective crisis management frameworks in the field of cybersecurity," among other fields for inter-institutional collaboration. Member States and involved EU institutions, bodies and agencies (EUIBAs) commit to "test[ing their] response to scenarios developed on the basis of regular EU risk assessment" once a year in the framework of an "annual dedicated Cyber Diplomacy Toolbox exercise." EU Member States have used the toolbox for diplomatic responses in support of third countries such as Georgia,[36] Ukraine,[37] the United Kingdom,[38] and Australia.[39] Many declarations and statements issued by the EU in this context make explicit references to the UN framework for responsible state behavior.

— Development of a regional posture on cyber defense

In addition, the EU has adopted several documents in the area of cyber defense, prescribing the roles and responsibilities of different institutions and mechanisms within the EU and at the national level.[40] In 2018, the EU identified cyberspace as a fifth domain of operations.[41] The EU's Military Vision and Strategy on Cyberspace as a Domain of Operations and the review of the Cyber Defence Policy Framework (CDPF), established in 2014 and updated in 2018 and 2022, are particularly relevant in this context. The latest 2022 EU Policy on Cyber Defence is built around four pillars aimed at (1) increasing information exchange and cooperation between military and civilian

34 Council of the EU (2017): Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 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 and Council of the EU (2023): Revised Implementing Guidelines of the Cyber Diplomacy Toolbox.

35 See also Cyber Diplomacy, in: Christina Rupp (2024): Navigating the EU Cybersecurity Policy Ecosystem: A Comprehensive Overview of Legislation, Policies and Actors, interface.

36 Council of the EU (2020): Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace.

37 Council of the EU (2022): Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine.

38 European External Action Service (2024): UK: Statement by the Spokesperson on recent malicious cyber activities.

39 Council of the EU (2024): Statement by the High Representative on behalf of the European Union, expressing solidarity with Australia on the impact of cyber-attacks against its health sector.

40 See also Cyber Defence, in: Christina Rupp (2024): Navigating the EU Cybersecurity Policy Ecosystem: A Comprehensive Overview of Legislation, Policies and Actors, interface.

41 Council of the EU (2018): Cyber defence: Council updates policy framework.

cybersecurity communities by reinforcing EU coordination mechanisms among national and EU cyber defense players, (2) protecting the defense sector from malicious cyber operations by introducing cybersecurity standardization and certification to secure both military and civilian domains, (3) improving cyber defense capabilities, and (4) setting up tailored partnerships in the area of cyber defense.[42] The EU tracks the implementation of its Policy on Cyber Defence through the Cyber Census annually, of which the executive summary is publicly available.[43]

At the institutional level, the European Defence Agency (EDA) is responsible for advancing the EU's cyber defense cooperation and supports Member States' capability development also in the area of cyber defense. For example, the EDA supports the creation of a risk management model for cybersecurity in the context of military capability supply chains, the establishment of the Cyber Ranges Federation project, as well as the development of specific capabilities for Advanced Persistent Threat (APT) detection and cyber situational awareness.[44] The EDA is also responsible for managing the Military Computer Emergency Response Team Operational Network (MICNET), which brings together military CSIRTs of EU Member States.[45]

— Articulation of a regional position on the applicability of international law in the cyber context

In 2024, the EU adopted a Declaration on a Common Understanding of International Law in Cyberspace. The declaration directly implements norm a as well as the normative framework as a whole. Through the declaration, the "EU and its Member States reaffirm their full commitment to, and stress the importance of the full implementation of, the United Nations framework of responsible State behaviour in cyberspace, adopted by consensus by the United Nations General Assembly, which affirms inter alia that, international law, in particular the UN Charter, international human rights law and international humanitarian law, fully applies to cyberspace." The declaration further elaborates the EU's view on how specific principles and rules of international law apply in the cyber context, such as the principles of state sovereignty and non-intervention or the prohibition of the use of force.

42 European Commission (2022): EU Policy on Cyber Defence.

43 European External Action Service (2025): EU Cyber Census 2025.

44 European Defence Agency (n.d.): Cyber.

45 European Defence Agency (2023): EDA-led network of cyber defence teams starts with 18 EU countries.

— Involvement in bilateral, regional, and multilateral cooperation at technical, operational, and diplomatic levels

Additional important cooperation mechanisms are cyber dialogues between the EU and key international partners, including Brazil, China, India, Japan, South Korea, Ukraine, the United Kingdom, and the United States. These dialogues are used to advance cooperation in areas such as cyber diplomacy, crisis management, capacity building, or cybersecurity of critical infrastructure. Certain elements of cyber diplomacy and norms implementation are also discussed in non-cyber specific formats such as bilateral Digital Partnerships and Digital Dialogues, as well as the EU-LAC Digital Alliance and the EU-Western Balkans Regulatory Dialogue. These engagements contribute to norms implementation through addressing topics such as trusted connectivity and resilience of digital infrastructures.

Since 2024, and as of July 2026, the EU has signed 12 security and defence partnerships with Moldova, Norway, Japan, South Korea, North Macedonia, Albania, the United Kingdom, Canada, India, Iceland, Australia, and Ghana.[46] The provisions of all of these partnerships also underscore a mutual commitment to multilateral, regional, and bilateral cooperation on cybersecurity governance.[47]

At the regional level, the EU maintains a partnership with the Organization for Security and Co-operation in Europe (OSCE), which contributes to the maintenance of international peace and security particularly through its 16 agreed cyber CBMs. As a "CBM adopter," the EU together with three OSCE participating states is especially driving the implementation of CBM 12 that prescribes to "act jointly to reduce tensions."[48]

In terms of cross-regional partnerships, the EU and NATO are holding an annual structured dialogue to enhance their collaboration.[49] The European Commission and ENISA also participate in the G7 Cybersecurity Working Group.[50] The EU is also part of the ASEAN Regional Forum, where it is involved, inter alia, in the development and implementation of cyber CBMs.[51]

46 Council of the EU (n.d.): Security and defence partnerships.

47 For example, European External Action Service (2026): Security and Defence Partnership between the European Union and the Commonwealth of Australia.

48 All EU Member States are also OSCE Participating States and many have assumed responsibility for CBMs under the Adopt-a-CBM initiative and finance capacity building activities in this context. Australia, Fiji, North-Macedonia, Poland, Switzerland, Inter-American Committee against Terrorism of the Organization of American States, and Transnational Threats Department of the Secretariat of the Organization for Security and Co-operation in Europe (2025): Inter-regional Cooperation The Role of Regional Organizations in Implementing the UN Framework for Responsible State Behaviour in Cyberspace.

49 European External Action Service (2025): Second EU-NATO Structured Dialogue on Cyber and European External Action Service (2024): European Union and NATO hold the first Structured Dialogue on Cyber.

50 Agenzia per la cybersicurezza nazionale (n.d.): G7 Cybersecurity Working Group.

51 Helene Pleil (2025): The State of Cyber Confidence-Building Measures: How Governments Implement Multilateral Measures to Create

These platforms are also used for strengthening cooperation regarding most recent technological developments. In addition to several concrete measures addressing the risks posed by frontier AI models, the EU Action Plan on Cybersecurity and Artificial Intelligence presented in July 2026 highlights the importance of international cooperation to avoid fragmentation, promote interoperability, and pool efforts to mitigate cybersecurity risks associated with AI.[52] It explicitly mentions the existing digital partnerships, digital dialogues, or cyber dialogues as instruments to deepen exchanges with partner countries on advanced AI and cybersecurity.

Enhancing interstate cooperation on cybersecurity is a core responsibility of the European External Action Service (EEAS), the EU's diplomatic service with a network of delegations around the globe. The EEAS plays a central coordination role in the EU's external action, supporting the High Representative and ensuring consistency between EU policies and Member States' diplomatic efforts. This includes fostering multilateral and cross-regional engagement, such as representing the EU in the Global Mechanism and convening dialogues with other regions. The EEAS is also involved in coordinated crisis response through mechanisms such as the EEAS Crisis Response Mechanism and its role in the application of the Union's Cyber Diplomacy Toolbox.

In 2023, the European cybersecurity agency ENISA concluded working arrangements with authorities in Ukraine[53] and the United States, which it continues to maintain.[54]

Considering all relevant information in case of ICT incidents (Norm B)

In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions, and/or partnerships in place to gather, analyze, and share information about cyber threats, actors and their tactics, techniques, and procedures?

Trust in the Cyber Domain, interface.

52 In addition, ENISA has published its view on cybersecurity in the "frontier AI area," offering an initial set of recommendations towards developing the necessary operational capabilities across the EU to face machine-speed threats, ENISA (2026): ENISA's view on Cybersecurity in the Frontier AI Era.

53 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.

54 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 cybersecurity.

- Q2: Does the EU have a clearly defined attribution policy to ensure that all relevant information is considered?
- Q3: Does the EU have a clearly defined approach to engaging with international partners, including a state suspected of conducting a malicious cyber activity?

Examples of activities that support the objective of considering all relevant information in case of ICT incidents:

- Designating national CSIRTs, inter alia, responsible for detecting and responding to ICT incidents;
- Establishing regional technical and operational information-sharing mechanisms, including between national CSIRTs;
- Introducing incident reporting obligations;
- Developing capabilities for coordinated regional and intraregional detection and situational awareness of ICT incidents;
- Articulating a national/regional approach to attribution, including the possible pursuit of joint regional attribution;
- Seeking the peaceful settlement of disputes arising from ICT incidents; and
- Adopting guidance on the classification of ICT incidents.

The following sections provide an overview of the EU's approach to implementing these activities. It should be noted that the political nature of attribution implies that it remains the sole prerogative of individual Member States and they must act unanimously for the EU as a whole to proceed with attribution.

— Designation of national CSIRTs, inter alia, responsible for detecting and responding to ICT incidents

Under the NIS2 Directive – and previously under its predecessor, the NIS1 Directive from 2016 – EU Member States are required to establish or designate at least one national CSIRT. The Directive also specifies their tasks, including "collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity."[55] This ensures that Member States have dedicated institutional capacity to consider all relevant information in the context of ICT incidents, including forensic evidence and the broader operational context.

55 Article 11(3) of the NIS2 Directive.

— Establishment of regional information-sharing mechanisms, including between national CSIRTs

The EU has put in place a range of regional information-sharing mechanisms at the technical and operational levels that enable the incorporation of multiple sources of information into the assessment of ICT incidents. The EU's Cyber Posture also stresses the importance of improving the EU's information-sharing mechanisms between relevant bodies to improve understanding of the cyber threat landscape, including through regular engagements with the private sector. ENISA contributes, inter alia, by producing regular EU cybersecurity situation reports, which aim to support a shared understanding of the threat landscape.[56] The CSIRTs Network facilitates the exchange of information between EU Member States' national CSIRTs on incidents, cyber threats, risks, and vulnerabilities, enabling authorities to draw on inputs from multiple national and technical sources when assessing an incident.[57] To support the response to large-scale incidents, the EU has also established a cyber crisis liaison organization network for the national authorities of Member States in charge of cyber crisis management: EU-CyCLONe. The network supports common situational awareness and the assessment of the consequences and impacts of cybersecurity crises.[58] CERT-EU also contributes by sharing information on incidents, threats, vulnerabilities, and near misses relevant to EU institutions.[59] Furthermore, the EEAS, including through structures such as EU INTCEN[60] and the Hybrid Fusion Cell, is equipped to provide additional analytical input

— Enactment of incident reporting obligations

The EU has established obligations for various entities to report incidents to national competent authorities and/or CSIRTs. This is important for the implementation of norm b because incident-related data from multiple sectors and jurisdictions can improve the completeness and reliability of the information available during the assessment of an incident. The NIS2 Directive prescribes that essential or important entities belonging to 18 sectors (see also Table 1 in Chapter 4.7), including public administration bodies, must notify a significant incident and provide specific information over particular timeframes. The required information should enable EU Member States to determine any cross-border impact of the incident.

---

56 ENISA (2026): Threat landscape.

57 See CSIRTs Network.

58 See EU-CyCLONe.

59 See also European Commission (2022): Call for tenders CNECT/2022/OP/0088 - Bespoke service to support the cyber situation and analysis centre for the European Commission and Leonardo (2023): First Pan-European Cyber Analysis Centre Now Operational.

60 The EEAS hosts the EU Intelligence and Situation Centre (EU INTCEN) and the EUMS' Intelligence Directorate (EUMS INT). EU INTCEN is a civil analysis unit within the EEAS, that processes intelligence received from Member States and other publicly accessible information. Unlike national intelligence services in EU Member States, EU INTCEN, has no independent operational intelligence-gathering capabilities. The EUMS INT represents the EU INTCEN's military counterpart. Together with the EUMS INT, INTCEN forms the Single Intelligence Analysis Capacity (SIAC).

Upon assessing an incident's significance, EU Member States shall, where appropriate, inform other EU Member States and ENISA of the incident, especially when the significant incident concerns two or more Member States.[61] National Single Points of Contact must share a summary report with ENISA every three months.[62] This report shall include "anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified."[63] In turn, ENISA is tasked with briefing the NIS Cooperation Group and the CSIRTs Network about its findings on notifications twice a year.[64] Apart from incident reporting obligations, EU Member States shall also encourage the voluntary exchange of information[65] among essential and important entities "through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared."[66]

Other information-sharing and incident reporting rules for specific sectors exist in the framework of the Critical Entities Resilience Directive, the Digital Operational Resilience Act and the Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows. The EUIBAs Regulation establishes similar rules for the reporting of incidents within EUIBAs to CERT-EU.

— Development of capabilities for coordinated regional and intraregional detection and common situational awareness of ICT incidents

In order to be able to consider all relevant information, states must have the capacity to detect ICT incidents and possess comprehensive situational awareness. Even though it remains primarily a national competence, the EU has introduced legislation to help accelerate this objective. The EU's Cyber Solidarity Act (CSOA) seeks to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents. One of its measures includes the establishment of a Cybersecurity Alert System, which is a pan-European network of infrastructure that consists of National Cyber Hubs and Cross-Border Cyber Hubs[67] with the objective of enhancing capabilities

61 Art. 23(6) NIS2 Directive.

62 Art. 23(9) NIS2 Directive.

63 Art. 23(9) NIS2 Directive.

64 Art. 23(9) NIS2 Directive.

65 Information in this respect, for instance, relates to "information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks." See Art. 29(1) NIS2 Directive.

66 Art. 29(2) NIS2 Directive.

67 To the knowledge of the authors, three cross-border cyber hubs had been established by May 2026: the Nordic-Baltic Cyber Consortium (NBCC; Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, and Norway; Sweden is expected to join the consortium at a later stage), the European Network of Security Operation Centers (ENSOC; Austria, Italy, Luxembourg, the Netherlands, Portugal, Romania, Slovenia, and Spain), and the europeAn THreat intelligence, rEspoNse and prepAredness (ATHENA; Bulgaria, Cyprus, Greece, and Malta), Estonian Information System Authority (2026): What to expect in cyberspace in 2026, Cyber Incident Response Institution of the Republic

for coordinated detection and common situational awareness, inter alia, by "pool[ing] relevant data and information on cyber threats and incidents." This collaboration within and across cross-border cyber hubs can support states in developing a more comprehensive and contextual understanding of ICT incidents, as called for in norm b. Designating a national cyber hub and participating in a cross-border cyber hub is voluntary for EU Member States.

— Articulation of a regional approach to attribution, including the possible pursuit of joint regional attribution

The Cyber Diplomacy Toolbox outlines the EU's approach to attribution, which remains a sovereign political decision of each Member State. Even though every Member State makes its own determination with respect to the attribution of malicious cyber activity, this understanding at the EU level is central to allow Member States to take (joint) action. Importantly, the CDT does not attempt to harmonize different methods, procedures, definitions, and criteria for attribution at the national level. Instead, it aims to facilitate the decision-making process at the EU level, including collective assessment of information and developing a shared situational awareness. Measures that are ultimately taken in response to malicious cyber activity also depend on the degree of certainty that can be established in a particular case. In cases where the Member States reach a shared assessment of the situation, they might proceed with a collective attribution and/or coordinate an attribution statement. Available tools also comprise the issuance of diplomatic démarches.[68]

The CDT's implementing guidelines provide further details about the EU's approach to attribution.[69] When discussing the appropriateness of coordinating political attribution and whether it should be done privately or publicly, the EU takes into account the following elements:[70]

- "[…] desired effect of the political attribution contribution to the protection of the integrity and security of the EU, its Member States and their citizens and businesses;
- importance of showing unity within the EU and between its Member States or solidarity with a third party;
- contribution to the advancement of responsible state behaviour, including compliance with international law and respect for voluntary norms;

of Latvia (2026): CERT.LV launches two new projects to strengthen cybersecurity, ENSOC - European Network of Security Operation Centers (n.d.): About and europeAn THreat intelligence, rEspoNse and prepAredness (n.d.): About.

68 Diplomatic démarches by EU Delegations or Member States represented in countries where malicious cyber activities originate from can jointly contact States exercising jurisdiction over these territories. The advantages of such démarches include raising concerns about certain malicious activities, signaling the seriousness of the incident to the EU, facilitating the peaceful resolution of an ongoing incident, and asking for assistance or cooperation to mitigate the malicious activity without resorting to formal (public) attribution.

69 Council of the EU (2023): Revised Implementing Guidelines of the Cyber Diplomacy Toolbox. An example of a past EU attribution is Council of the EU (2022): Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union.

70 Council of the EU (2023): Revised Implementing Guidelines of the Cyber Diplomacy Toolbox.

- ability to influence the behaviour of malicious actors in cyberspace;
- impact on the ongoing work of services such as law enforcement or intelligence services;
- likelihood and impact of a counter-response by any actor (risk of escalation);
- consequences for existing EU external relations, at the international, regional and bilateral levels;
- reputation and credibility of the EU (risk of the bystander effect, risk of manipulation, precedence of a malicious cyber activity);
- predictability and coherence of joint EU responses in previous and/or future cases."

Although the EU recognized that there is no international legal obligation to reveal evidence on which attribution is based prior to taking an appropriate response, the EU does acknowledge that attribution should be based on an analysis of technical data and all-source intelligence, including the possible interests of the perpetrator. The decision-making process for responding on the basis of an attribution made by one or more EU Member States is discussed in the Horizontal Working Party on Cyber Issues. It also involves the Council's Political and Security Committee if political guidance is needed, other regional and thematic Council working groups if required, and the Foreign Relations (RELEX) Counsellors Working Party in cases where the EU may opt for imposing restrictive measures. The Court of Justice of the EU plays an important role in ensuring that the addressees of the EU measures (especially sanctions) have received all the necessary information and that the process has followed the rule of law standards.

— Recognition of the need to seek the peaceful settlement of disputes arising from ICT incidents

In addressing responses to an malicious ICT activity attributable to another state, the 2024 EU Declaration on a Common Understanding of International Law in Cyberspace emphasizes that "the parties to any dispute, especially if the continuance of that dispute is likely to endanger the maintenance of international peace and security, shall seek a solution by peaceful means [as reflected in Articles 2(3) and 33(1) of the UN Charter]. Peaceful means include diplomatic measures, recourse to negotiation, mediation, conciliation, arbitration, judicial settlement or any other peaceful means of dispute resolution of their own choice."

— Adoption of guidance on the classification of ICT incidents

The implementation of this norm is also supported by the 2018 Cybersecurity Incident Taxonomy of the EU's NIS Cooperation Group, which categorizes the root cause and severity of threats in terms of the nature of the incident, as well as the affected sectors, scale, and outlook, to evaluate the incident's impact. This taxonomy can help authorities assess "the severity and replicability of an ICT incident," as mentioned in the 2021 OEWG guidance as a means of operationalization.[71]

Preventing misuse of ICTs (Norm C)

States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions, and/or partnerships in place to monitor adverse activities using ICTs within its territory?
- Q2: If an internationally wrongful act occurs within the EU's territory, are there policies and institutions to mitigate or contain the ongoing activity in its territory?

Examples of activities that support the objective of preventing the misuse of ICTs in a state's territory:

- Designating national CSIRTs inter alia, responsible for detecting and responding to ICT incidents;
- Establishing regional information-sharing mechanisms, including between national CSIRTs;
- Developing capabilities for coordinated regional and intraregional detection and situational awareness of ICT incidents;
- Criminalizing wrongful acts involving the misuse of ICTs;
- Adopting standards and procedures concerning the export of cyber-surveillance tools;
- Articulating a national/regional understanding of the applicability of the principle of due diligence in the cyber context.

The following sections provide an overview of the EU's approach to implementing these activities.

— Designation of national CSIRTs, inter alia, responsible for detecting and responding to ICT incidents

Under the NIS2 Directive, EU Member States are required to establish or designate at least one national CSIRT (see also the section on norm b). This obligation supports norm c by mandating states to build the institutional and technical capacities necessary to detect, analyze, and respond to adverse cyber activities originating from or transiting through their territory.

71 United Nations General Assembly (2021): Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

— Establishment of regional information-sharing mechanisms, including between national CSIRTs

The EU's information-sharing and situational awareness actors and mechanisms (including those discussed in the section on norm b) support the aggregation and exchange of technical, operational, and intelligence information relevant to adverse cybersecurity events and incidents. They also provide options for joint response action through Union crisis frameworks. These established channels of trusted information-sharing and cooperation can contribute to reducing the likelihood that malicious ICT activities originating from or transiting through Member States' territory remain unnoticed and ultimately unaddressed.

— Development of capabilities for coordinated regional and intraregional detection and common situational awareness of ICT incidents

Fulfilling the due diligence obligation contained in this norm presupposes sufficient detection capacity and cooperation with actors such as internet service providers and other relevant entities, so that states can either detect internationally wrongful acts originating from their territory themselves or be informed by others. As discussed in more detail in the section on the EU's implementation of norm b, the EU Cyber Solidarity Act seeks to enhance the Union's overall capabilities in this regard, inter alia, through the establishment of a Cybersecurity Alert System, a pan-European network of infrastructure that consists of National Cyber Hubs and Cross-Border Cyber Hubs.

— Criminalization of wrongful acts involving the misuse of ICTs

The primary aim of norm c is to ensure that states put in place mechanisms – regulatory and institutional – that would prohibit any internationally wrongful activities from originating in EU territory. In the EU context, this has been primarily done by criminalizing misuse of ICTs (see further the section on norm d) as well as putting in place the necessary institutional framework that would strengthen the awareness of the EU and Member State agencies about cyber activities in the EU territory – both those originating inside and outside.

— Adoption of standards and procedures concerning the export of cyber-surveillance tools

Another dimension of ensuring that territories are not used for malicious activities against

other states is reflected in the adoption of concrete standards and procedures, for instance, regarding trade in dual use goods or the production and exports of cyber surveillance tools. To that effect, the EU's export control regime[72] puts in place a comprehensive framework of regulations and institutions to ensure common export control rules, including a common set of assessment criteria and common types of authorizations (individual, global and general authorizations). In addition, the EU General Export Authorizations (EUGEAs) apply to exports of dual-use items to certain destinations under certain conditions, including telecommunications, intra-group technology transfers, and encryption.[73]

— Articulation of a regional understanding of the applicability of the principle of due diligence in the cyber context

There are limited EU policy documents explicitly mentioning the due diligence principle. Most importantly, the EU's 2024 Declaration on a Common Understanding of International Law in Cyberspace reaffirms its applicability in the cyber context. Referencing the International Court of Justice's 1949 Corfu Channel judgment, EU Member States note the following: "as States have jurisdiction over ICT infrastructure and individuals as referred to in Section 1 above [Section 1 discusses the principle of state sovereignty], they are required to make efforts that this ICT infrastructure is not used by non-State or State actors for acts contrary to the rights of other States, once they know or ought to have known of such activities. States are required to take all appropriate and reasonably available and feasible measures, in the given context, to act against cyber operations that violate rights of another State under international law. The same duty applies for cyber activities within the territory or ICT infrastructure that they otherwise effectively control. If a State does not act with due diligence in relation to cyber activities within or using ICT infrastructure located in its territory, it may commit an internationally wrongful act. At the same time, the due diligence obligation does not require preventive monitoring of all cyber activities and ICT infrastructure in the territory of a State or within its effective control."

Already earlier in 2018, EU Member States had highlighted the importance of "not us[ing] proxies to commit internationally wrongful acts using ICTs, and [that states] should seek to ensure that their territory is not used by non-state actors to commit such acts" in their Council Conclusions on malicious cyber activities.

72 See also European Commission (n.d.): Exporting dual-use items.

73 Regulation 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

Cooperation to stop use of ICTs for crime and terrorism (Norm D)

States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions, and/or partnerships in place that support cooperation at political and operational levels to prosecute terrorist and criminal use of ICTs?
- Q2: Does the EU have mechanisms in place to exchange information with and assist other states to cooperate on addressing terrorist and criminal use of ICTs?

Examples of activities that support the objective of cooperating across borders to stop the use of ICTs for criminal and terrorist purposes:

- Developing a national/regional framework for the criminalization of wrongful acts involving the misuse of ICTs;
- Developing a national/regional framework to prevent the use of ICTs for terrorist purposes;
- Establishing national/regional law enforcement institutions and coordination structures to cooperate to stop cybercrime;
- Adopting rules to facilitate practical cooperation between judicial and law enforcement authorities;
- Participating in and promoting international instruments to fight criminal and terrorist use of ICTs.

The following sections provide an overview of the EU's approach to implementing these activities.

— Development of a regional framework for the criminalization of wrongful acts involving the misuse of ICTs

The EU implements norm d by putting in place a legal framework that aims to improve the prevention, investigation, and prosecution of cybercrime and child sexual exploitation, strengthens capacity across the criminal justice system, and creates modalities for cooperation with industry. The origins of this framework date back to the early 1990s when the discussions about ICT and information security first emerged and therefore predate the formal institutionalization of norm d.

The EU's legal framework to fight the criminal use of ICTs focuses primarily on three broad categories of crimes:[74]

- Crimes specific to the internet: The EU's 2013 Directive on attacks against information systems aims to tackle large-scale malicious cyber activity by criminalizing core offences including illegal access to information systems, illegal system interference, illegal data interference, and illegal interception, as well as the production, sale, or distribution of tools designed to commit these offences, and the incitement, aiding, and abetting of such conduct. It also establishes cooperation obligations for Member States, requiring them to designate an operational national point of contact, using a 24/7 network for information sharing on offences, and responding to urgent requests for assistance in a timely manner.
- Online fraud and forgery, through instruments such as identity theft, phishing, spam and malicious code: In 2019, with the Directive on combating fraud and counterfeiting of non-cash means of payment, the EU updated its legal framework to remove obstacles to operational cooperation, enhance prevention and victims' assistance, and make law enforcement action against fraud and counterfeiting of non-cash means of payment more effective.
- Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia: In 2011, the EU adopted the Directive on combating the sexual exploitation of children online and child pornography.

— Development of a regional framework to prevent the use of ICTs for terrorist purposes

To address the challenges posed by the dissemination of terrorist content online, the EU adopted Regulation 2021/784. The Regulation aims to ensure the smooth functioning of the digital single market in an open and democratic society by addressing the misuse of hosting services for terrorist purposes and contributing to public security across the EU. For example, any hosting service provider offering its services in the EU must take active steps to remove terrorist content on its platforms within one hour, once they are alerted by national competent authorities. The law stresses the importance of ensuring that any such efforts need to strengthen safeguards to the freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society and the freedom and pluralism of the media.

— Establishment of regional law enforcement actors and co-ordination structures to cooperate to stop cybercrime

The EU's legal and policy framework is accompanied by a robust institutional architecture. At the center of this system is Europol's European Cybercrime Centre (EC3), set up in 2013 to bolster the response of law enforcement to cybercrime in the EU and help protect European citizens, businesses and governments.[75] The EC3 offers

74 European Commission (2024): Cybercrime.

operational, strategic, analytical and forensic support to Member States' investigations. It performs several functions, such as:

- serving as the central hub for criminal information and intelligence;
- supporting operations and investigations by Member States by offering operational analysis, coordination, and expertise;
- providing highly specialized technical and digital forensic support capabilities to investigations and operations;
- offering support to EU crisis management structures, within the scope of Europol's mandate, and facilitating the operational, technical and strategic collaboration between law enforcement agencies (LEAs) and other relevant cyber communities and EU institutions, bodies and agencies (e.g. Eurojust, EEAS, ENISA, CERT-EU, Commission, Council, etc.);
- delivering 24/7 operational and technical support to LEAs for immediate reaction to urgent cyber incidents and/or cyber crises via stand-by duty and the EU Law Enforcement Emergency Response Protocol (EU LE ERP);[76]
- supporting training and capacity building;[77]
- producing a variety of strategic analysis products that enable informed decision-making on combating and preventing cybercrime;
- maintaining a comprehensive outreach function connecting law enforcement authorities tackling cybercrime with the private sector, academia and other non-law enforcement partners.

The EC3 publishes an annual Internet Organised Crime Threat Assessment (IOCTA).[78] The EC3 also hosts the Joint Cybercrime Action Taskforce (J-CAT) whose mission is to drive intelligence-led, coordinated action against key cybercrime threats through cross-border investigations and operations by its partners.[79] J-CAT brings together representatives of EU Member States as well as other third countries and also cooperates with the private sector. J-CAT has conducted several high-profile operations aimed at dismantling cybercrime networks and infrastructure (see further the section on norm d).

Alongside Europol, other EU agencies play important roles in judicial and operational cooperation on cybercrime. The EU established the European Union Agency for Criminal Justice Cooperation (Eurojust) in 2002 to support the coordination of cross-border criminal investigations and prosecutions, including in cybercrime cases. It facilitates information exchange, linking national investigations, and promotes joint investigative action. Eurojust also contributes to strategic and legal analysis through publications such as the Cybercrime Judicial Monitor and supports practitioner cooperation through the European Judicial Cybercrime Network.[80] Meanwhile, eu-LISA, established in 2011,

75 Europol (n.d.): European Cybercrime Centre - EC3.
76 Europol (2019): Law enforcement agencies across the EU prepare for major cross-border cyber-attacks.
77 Europol (2025): Training and capacity building.
78 Europol (n.d.): Internet Organised Crime Threat Assessment (IOCTA).
79 Europol (n.d.): Joint Cybercrime Action Taskforce (J-CAT).
80 Eurojust (n.d.): Cybercrime Judicial Monitor and Eurojust (n.d.): European Judicial Cybercrime Network.

manages the EU's large-scale IT systems supporting the Area of Freedom, Security and Justice and contributes to internal security through platforms such as the Joint Investigation Teams Collaboration Platform and e-CODEX.

In addition, the EU has developed several collaborative mechanisms to enhance coordinated action against cybercrime and organized crime. The European Union Cybercrime Task Force (EUCTF) functions as a network of national cybercrime units, EU institutions, and associated non-EU countries (currently Denmark, Iceland, Norway, Switzerland, and the United Kingdom), aiming to promote a harmonized EU approach to combating cybercrime and identifying common operational priorities.[81] The EU has also established the European Multidisciplinary Platform Against Criminal Threats, EMPACT, for combating serious and organized international crime through four-year policy cycles.[82] EMPACT brings together Member States, EU agencies as well as associated third countries, international organizations, and private-sector partners. The current 2026-2029 EMPACT cycle identifies cyberattacks, online child sexual exploitation, and online fraud among its key priorities.

— Adoption of intraregional rules to facilitate practical cooperation between judicial and law enforcement authorities

The EU has also taken steps to facilitate practical cooperation between judicial and law enforcement authorities within the EU. This includes rules for cross-border access to electronic evidence in accordance with fundamental rights, privacy, and due process. Through the e-evidence package, the EU has introduced measures aimed at "mak[ing] it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals."[83]

In that regard, Regulation 2023/1543 introduced two new cooperative mechanisms at the EU level:

- a European Production Order that allows a judicial authority in one Member State to obtain electronic evidence (such as emails, text or messages in apps, as well as information to identify a perpetrator as a first step) directly from a service provider or its legal representative in another Member State;
- a European Preservation Order that allows a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserve specific data in view of a subsequent request to produce this data via mutual legal assistance, a European Investigation Order or a European Production Order.

Other EU legislation supports cross-border cooperation through additional instruments. They include a voluntary Joint Investigation Teams collaboration platform to facilitate

81 Europol (2024): European Union Cybercrime Task Force.
82 European Commission (2025): EMPACT fighting crime together.
83 European Commission (n.d.): E-evidence - cross-border access to electronic evidence.

cooperation between competent authorities, including in cybercrime cases[84] and the e-CODEX system,[85] which enables secure electronic exchange of data in civil and criminal judicial cooperation.

— Participation in and promotion of international instruments to fight criminal and terrorist use of ICTs

To a large extent, the EU's approach on international cooperation in the area of cybercrime is built around different provisions of the Council of Europe Convention on Cybercrime (Budapest Convention), which the EU supports as the main international instrument to guide cooperation at the international level.[86] All EU Member States are parties to the Budapest Convention. In October 2025, the EU signed the UN Convention against Cybercrime.[87]

To tackle specific forms of cybercrime and terrorist use of ICTs through international cooperation, the EU participates in several multilateral initiatives. The EU is a member of the International Counter Ransomware Initiative (CRI), which seeks to strengthen global cooperation against ransomware operations through coordinated policy responses, information-sharing, and capacity building.[88] The European Commission is a supporter of the Christchurch Call to eliminate terrorist and violent extremist content online.[89]

Respecting human rights and privacy (Norm E)

States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions, and/or partnerships in place to ensure the promotion, protection, and enjoyment of human rights online, including the right to privacy in the digital age and the right to freedom of expressions?

84 Regulation 2023/969 establishing a collaboration platform to support the functioning of joint investigation teams.

85 Regulation 2022/850 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system).

86 Council of Europe (n.d.): Details of Treaty No.185 (Convention on Cybercrime).

87 United Nations Treaty Collection (2026): United Nations Convention against Cybercrime and Council of the EU (2025): Fighting cybercrime: EU to sign UN Convention on cybercrime.

88 International Counter-Ransomware Initiative (n.d.): About the CRI.

89 The Christchurch Call (n.d.): Supporters.

Examples of activities that support the objective of respecting human rights and privacy in the digital age:

- Adopting policies and establishing institutions that promote and protect human rights and fundamental freedoms online and offline;
- Enacting data protection legislation ensuring respect for the right to privacy in the digital age;
- Adopting legislation governing the use of personal data for law enforcement purposes;
- Establishing standards and procedures to ensure compliance with human rights obligations when cyber-surveillance items are exported; and
- Articulating a regional position on the applicability of international human rights law in the cyber context.

The following sections provide an overview of the EU's approach to implementing these activities.

— Commitment to the promotion and protection of human rights and fundamental freedoms online and offline

The EU Cybersecurity Strategy states clearly that the EU should lead on the protection and promotion of human rights and fundamental freedoms online. To this end, the EU seeks to promote further compliance with international human rights law and standards, as well as operationalizing its Action Plan on Human Rights and Democracy for years 2020-2027, and advance its Human Rights Guidelines on Freedom of Expression Online and Offline.[90] Furthermore, the strategy stresses that the EU should make sustained efforts to protect human rights defenders, civil society and academia working on issues such as cybersecurity, data privacy, surveillance and online censorship.

At the core of the EU's approach is the commitment to the right to protection of their personal data and putting in place robust legal and institutional framework to protect privacy of the EU citizens. The right to privacy is explicitly listed in the EU Charter of Fundamental Rights and in the European Declaration on Digital Rights and Principles, which "puts people at the centre, in line with EU values and fundamental rights." The Court of Justice of the European Union and the European Court of Human Rights are important players in the EU's legal landscape in that they ensure respect for the existing international human rights regime by individual Member States.

90 European External Action Service (2020): EU Action Plan on Human Rights and Democracy 2020 – 2024 and Council of the EU (2014): EU Human Rights Guidelines on Freedom of Expression Online and Offline.

— Enactment of data protection legislation ensuring respect for the right to privacy in the digital age

At the center of the EU's legal framework is the General Data Protection Regulation (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The regulation is an essential step toward strengthening individuals' fundamental rights in the digital age and facilitating business by clarifying rules for companies and public bodies operating in the digital single market.[91]

At the institutional level, the European Data Protection Supervisor (EDPS) serves as an independent EU body responsible for monitoring the application of data protection rules within European institutions and for investigating complaints.[92] In addition, the European Data Protection Board (EDPB) is an independent European body established to ensure the consistent application of data protection rules throughout the EU. The EDPB is composed of representatives from the national data protection authorities of the EU/EEA countries and the EDPS. The EDPB tasks consist primarily in providing general guidance on key concepts of the GDPR and the Data Protection Law Enforcement Directive (see below), advising the European Commission on issues related to the protection of personal data and new proposed legislation, and adopting binding decisions in disputes between national supervisory authorities.

— Adoption of legislation governing the use of personal data for law enforcement purposes

The Data Protection Law Enforcement Directive protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes. It particularly aims to ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and facilitate cross-border cooperation in the fight against crime and terrorism.[93]

91 See also European Commission (2024): Reports on the application of GDPR.
92 European Data Protection Supervisor (n.d.): About Us.
93 Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

— Establishment of standards and procedures to ensure compliance with human rights obligations when cyber-surveillance items are exported

The EU addresses the importance of upholding human rights obligations also in the context of its export control regime of dual-use items. As a particular category of these dual-use items, the Regulation includes 'cyber-surveillance items,' which it defines as "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems."[94] As a general rule, all items contained in Annex I of the Regulation require prior authorization. Annex I specifies ten categories of items in detail, one titled telecommunications and information security (category five).

Concerning cyber-surveillance items not included in Annex I, export authorization is required "if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law."[95] Exporters themselves shall notify their respective competent authority in EU Member States, if they are "aware, according to [their] due diligence findings" that the proposed export of such items may "in their entirety or in part" serve any of the above-mentioned use cases. On that basis, Member States, via their competent authorities, "shall decide whether or not to make the export concerned subject to authorisation."[96] To help exporters make such determinations, the Commission has published non-binding guidelines in 2024.[97]

— Articulation of a regional position on the applicability of international human rights law in the cyber context

The EU's 2024 Declaration on a Common Understanding of International Law in Cyberspace underscores the EU's commitment to promote and protect the enjoyment of human rights online. To that end, EU Member States highlight that "states must comply with their obligations under international human rights law online just as offline. States are under a negative obligation to refrain from acting in violation of human rights, as well as a positive obligation to actively protect the rights of persons within their jurisdiction

94 Art. 2, point (20) Regulation 2021/821.
95 Art. 5(1) Regulation 2021/821.
96 Art. 5(2) Regulation 2021/821.
97 Commission Recommendation 2024/2659 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation 2021/821. See also Federal Office for Economic Affairs and Export Control (2021): Leaflet on Art. 5 of the EU Dual-Use Regulation (Regulation (EU) 2021/821).

against such violations." In the same vein, EU Member States emphasize that their protection is especially important in the cyber context, where the freedom of opinion and expression, the right to privacy, the freedom to seek, receive, and impart information, the freedom of peaceful assembly and association, the prohibition of discrimination and the rights of the child "might be particularly at risk."

Not damaging critical infrastructure (Norm F)

A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions, and/or partnerships in place to address the use of ICT that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public?

Examples of activities that support the objective of not intentionally damaging critical infrastructure:

- Putting in place rules and processes for designating critical infrastructure sectors;
- Articulating a national/regional understanding on the applicability of international law in the cyber context;
- Developing a national/regional position and doctrine on cyber defense; and
- Establishing a cyber command and regional platforms for cooperation and information exchange between cyber commands and military CSIRTs.

Given that EU Member States have full competence over their national security, the EU's role in the implementation of the UN cyber norms of a prohibitive nature is rather limited. Nonetheless, the EU has taken certain measures that provide an overall framing for its Member States' behavior in cyberspace, including on aspects related to the objective of norm f. The following sections provide an overview of the EU's approach to implementing these activities.

— Regional designation of critical infrastructure sectors[98]

The NIS2 Directive and the Critical Entities Resilience (CER) Directive identify sectors of critical importance (see further section on norm g). While the designation of critical infrastructure and respective entities remains a national prerogative and there is no agreed upon international definition on what constitutes critical infrastructure, these instruments establish a shared EU-level baseline reference point that could also possibly indirectly be used to guide operators in EU Member States. For example, it could be helpful in cases where information on another state's critical infrastructure designation is not available, in determining which types of infrastructure could be considered off limits to cyber activities. In addition, the EU's statements issued following the operations targeting specific entities in Germany, Czechia, Ukraine, and Australia, to name a few, indicate what type of critical infrastructure the EU would consider to be off limits.[99]

— Articulation of a regional understanding on the applicability of international law in the cyber context

The 2024 EU Declaration on a Common Understanding of International Law in Cyberspace implements the commitment in an interpretative sense by providing contextual guidance to EU Member States on their obligations under international law. In laying out what may in turn constitute ICT activity contrary to such obligations as referred to in the norm, the declaration can support Member States in assessing what conduct – aimed at the critical infrastructure of other states as the specific scenario provided for – would potentially constitute a violation of norm g.

— Development of a regional posture on cyber defense

Cyber defense and the employment of related capabilities in the entire spectrum of military cyberspace operations is a national prerogative of Member States, while relying on a wider ecosystem, including a strong industrial base supported by EU-level capability development (see further also the explainer on cyber defense in Chapter 4.1). For example, the EU's Military Vision and Strategy on Cyberspace as a Domain of

98 Determinations on what constitutes critical infrastructure are also listed in the ASEAN Norms Implementation Checklist and a preceding UNIDIR paper mapping relevant implementation activities, ASEAN (2025): ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace and Samuele Dominioni and Giacomo Persi Paoli (2023): Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, UNIDIR.

99 Council of the EU (2024): Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation, Council of the EU (2025): Cyber: Statement by the High Representative on behalf of the European Union on malicious behaviour in cyberspace against Czechia, Council of the EU (2022): Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine, and Council of the EU (2024): Cyber: Statement by the High Representative on behalf of the European Union, expressing solidarity with Australia on the impact of cyber-attacks against its health sector.

Operations adopted in 2021 lays out the framework conditions and describes the ends and means needed to use cyberspace as a domain of operations in support of the EU's Common Security and Defence Policy (CSDP) operations.[100]

— Establishment of regional platforms for cooperation and information exchange between cyber commands and military CSIRTs

In recent years, several fora were established to enhance collaboration of the EU's cyber defense community, inter alia, as envisaged in the EU Policy on Cyber Defence (see further the section on norm a). In 2022, the EU inaugurated the Conference of European Cyber Commanders (CYBERCO), in which representatives of the cyber commands convene twice a year.[101] The EDA acts as CYBERCO's secretariat with the participation of the EU Military Staff. In addition, on a regular basis, the Cyber Commanders and Cyber Ambassadors of EU Member States meet in a joint conference or come together in other constellations.[102]

As far as military situational awareness is concerned, in 2026, the EU transformed the Cyber and Information Domain Coordination Centre Permanent Structured Cooperation in Security and Defence Policy (PESCO) project into a permanent EU Cyber Defence Coordination Centre (EUCDCC) to support enhanced situational awareness within the defense community, including all EU military CSDP commanders.[103] MICNET was established in 2022, supported by EDA. As MICNET reaches a higher level of maturity, EDA will support Member States in exploring options for collaboration with its civilian counterpart, the CSIRTs network.[104]

Protecting critical infrastructure (Norm G)

States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions, and/or partnerships in place to designate and protect its critical infrastructure from ICT threats?

100 European External Action Service (2021): European Union Military Vision and Strategy on Cyberspace as a Domain of Operations.
101 French General Secretariat for Defence and National Security (2026): National Cybersecurity Strategy 2026–2030.
102 Spanish Ministry of Defence (2025): Joint Cyber Command Participates in the Conference of Cyber Commanders and Cyber Ambassadors of EU member states and EU Cyber Direct (2024): EU Informal Meetings of Cyber Ambassadors and Cyber Commanders.
103 Benedikta von Seherr-Thoss (2026): LinkedIn Post, European Defence Agency (2025): LinkedIn Post and German Federal Ministry of Defence (2023): Cyber and Information Domain Coordination Centre (CIDCC).
104 European Commission and High Representative (2022): EU Policy on Cyber Defence.

Examples of activities that support the objective of protecting critical infrastructure:

- Designating critical infrastructure sectors and put in place procedures for identifying critical infrastructure entities;
- Establishing a regulatory framework for the protection of critical infrastructure;
- Introducing voluntary, coordinated preparedness testing for highly critical entities;
- Establishing regional platforms for cooperation and information exchange in the area of critical infrastructure protection;
- Adopting and testing critical infrastructure-specific crisis and incident management frameworks; and
- Maintaining and supporting the integrity and availability of critical Internet infrastructure.

The following sections provide an overview of the EU's approach to implementing these activities.

— Designation of critical infrastructure sectors and national identification of critical infrastructure entities

The EU's main legislative framework for the protection of critical infrastructure is the cross-sectoral NIS2 Directive which provides EU-wide legal measures to boost the overall level of cybersecurity in the EU. The NIS2 Directive is complemented by the Union's Critical Entities Resilience (CER) Directive, which, although not cyber-specific, is intended to be implemented in a coordinated manner with NIS2 in light of the interdependence between the physical security and cybersecurity of critical entities.[105] By expanding the scope of the cybersecurity rules to new sectors and entities, the two rulebooks contribute to strengthening resilience and incident response capacities in public and private sectors.

Both the NIS2 Directive and the CER Directive identify sectors of critical importance and impose obligations on Member States, as well as private and public actors within those sectors. While NIS2 distinguishes between sectors of high criticality and other critical sectors, the CER Directive provides a single category of critical sectors:

105 See also Commission Delegated Regulation 2023/2450 supplementing Directive 2022/2557 by establishing a list of essential services.

Legal Basis	Sectors
Sectors covered by both the NIS2 (“high criticality”) and CER Directives	• Energy • Transport • Banking • Financial market infrastructures • Health • Drinking water • Waste water • Digital infrastructure • Public administration • Production, processing and distribution of food (NIS2 lists this sector as critical, not highly critical)
Additional sectors covered by the NIS2 Directive	Highly critical: • Space Critical: • Postal and courier services • Waste management • Manufacture, production and distribution of chemicals • Production, processing and distribution of food • Manufacturing • Digital providers • Research

Table 1: Critical sectors as defined by the NIS2 and CER Directives

The Directives further specify criteria for Member States to determine which entities within these sectors are considered essential or important (under NIS2) or critical (under the CER Directive) and are therefore in scope. The CER Directive also provides for the designation of a subset of entities, so-called “critical entities of particular European significance,” which provide the same or similar essential services in six or more EU Member States and are subject to additional obligations.

— Establishment of a regional regulatory framework for the protection of critical infrastructure

For Member States, the NIS2 Directive requires measures such as a national cybersecurity strategy, a crisis management framework, a coordinated vulnerability disclosure policy, and systems for supervision and enforcement. The Critical Entities Resilience Directive requires Member States, inter alia, to adopt strategies to strengthen the resilience of critical entities, carry out risk assessments, identify critical entities, provide support, and ensure supervision through measures such as audits, inspections, and penalties. For the entities covered, NIS2 requires essential and important entities to implement particular governance and risk management measures and to report incidents. Similarly, the Critical Entities Resilience Directive requires critical entities to assess risks, strengthen their resilience, and report incidents.

In addition to these horizontal initiatives, the EU also mandates protective measures for specific sectors. For instance, in the financial sector, the Digital Operational Resilience Act (DORA) aims to strengthen the IT security of financial entities such as banks, insurance companies, and investment firms. DORA harmonizes rules related to cyber resilience for 21 different types of financial entities and ICT third-party service providers, with a scope that is more wide-ranging than that of the NIS2 and the Critical Entities Resilience Directive. DORA, inter alia, requires financial entities to implement comprehensive ICT risk management frameworks, including incident management and reporting, regular testing (such as vulnerability assessments and scans), and management of risks related to ICT third-party providers.

Furthermore, the EU has taken related legislative protective measures also in the area of electricity through a Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows mandating measures in the areas of risk management and incident reporting, among others. The civil aviation sector is also subject to comprehensive EU regulations to ensure its security.[106] Another example of a sector-specific risk assessment is the EU's recommendations for mitigating cybersecurity risks in telecommunications and electricity sectors. It highlights the importance of sharing good practices on mitigating ransomware, improving collective cyber-situational awareness and information sharing; improving contingency planning, crisis management and operational collaboration; assessing dependencies on high-risk third-country providers to strengthen supply chain security.[107]

But having legislation in place is just the beginning of the process. An interesting method to support the implementation of the norms through monitoring and accountability are reports on investments in the implementation of the NIS1 and 2 Directives.[108] These reports by ENISA offer a comprehensive overview of the state's investment in information security and human resources, which are critical for effective implementation of norm g.

— Introduction of voluntary, coordinated preparedness testing for highly critical entities

The EU Cyber Solidarity Act introduces several new institutional and procedural solutions of a cooperative nature. In the framework of its Cybersecurity Emergency

106 For example, Commission Implementing Regulation 2019/1583 amending Implementing Regulation 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures.

107 European Commission (2024): EU's recommendations for mitigating cybersecurity risks in telecommunications and electricity sectors published.

108 ENISA (2025): What's Driving Cybersecurity Investments and where lie the challenges?.

Mechanism, the Regulation puts in place procedures to voluntarily test entities in highly critical sectors under the NIS2 Directive such as finance, energy and health (to be identified by the European Commission) for potential weaknesses that could make them vulnerable to cyber threats with the objective of increasing the overall level of preparedness across the EU.[109] In practice, the Regulation lists penetration testing and threat assessments as possible preparedness-testing actions for which entities may receive financial support. In addition, support under the Cyber Solidarity Act is not limited to entities in the identified sectors but can also extend to preparedness actions for entities outside those designated for coordinated testing. Such support may include vulnerability and risk monitoring, exercises, and training, and can be provided to Member States under specific circumstances upon request.[110]

— Establishment of regional platforms for cooperation and information exchange in critical infrastructure protection

Both the NIS2 and Critical Entities Resilience Directives provide for an institutional set-up to enhance information-exchange between Member States and EUIBAs. The NIS2 Directive provides for the establishment of the NIS Cooperation Group, the CSIRTs Network and EU-CyCLONe. The NIS Cooperation Group's overall mission is to achieve a high common level of security for network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States.[111] The NIS Cooperation Group has delivered several guidelines and compendium documents, including guidelines on security measures for Top-Level-Domain Name Registries,[112] guidelines for the Member States on voluntary information exchange on cross-border dependencies,[113] a compendium on cybersecurity of election technology,[114] or the cybersecurity incident taxonomy.[115]

On the operational side, the NIS Cooperation Group is supported by the work of the network of Computer Security Incident Response Teams (CSIRTs Network), dedicated to sharing information about risks and ongoing threats as well as cooperating on specific cybersecurity incidents. The NIS Cooperation Group provides strategic guidance for the activities of the CSIRTs network.

In addition, the CER Directive establishes the Critical Entities Resilience Group (CERG), comprising representatives of EU Member States and the Commission. The Group is,

109 Art. 12 CSOA.

110 Art. 13 CSOA.

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

112 NIS Cooperation Group (2022): Technical Guideline: Security Measures for Top-Level-Domain Name Registries.

113 NIS Cooperation Group (2019): Guidelines for the Member States on voluntary information exchange on cross-border dependencies.

114 NIS Cooperation Group (2018): Compendium on Cyber Security of Election Technology.

115 NIS Cooperation Group (2018): Cybersecurity Incident Taxonomy.

inter alia, mandated to "facilitat[e] the exchange of best practices with regard to the identification of critical entities by the Member States" and "exchang[e] best practices related to the notification of incidents."[116] The CERG and NIS Cooperation Group shall convene at least once annually for a joint meeting.

— Adoption and testing of critical infrastructure-specific crisis and incident management frameworks

In addition to its cyber-specific Cyber Blueprint and cyber crisis management-related provisions contained in the NIS2 Directive, the EU has adopted a Critical Infrastructure Blueprint in June 2024 to coordinate Union-level responses to disruptions of critical infrastructure with significant cross-border relevance. Where incidents affect both the physical and cybersecurity dimensions of critical infrastructure, the two frameworks are intended to be applied coherently to strengthen coordination and leverage synergies. Similar to the Cyber Blueprint, the Critical Infrastructure Blueprint seeks to contribute to shared situational awareness, coordinated public communication, and coordinated responses while clarifying the responsibilities of relevant actors at Member State and Union level and of existing coordination bodies, across operational, strategic, and political levels.

Both frameworks place particular emphasis on regular testing through exercises, including exercises aimed at testing their interplay. In addition, the Cyber Blueprint tasks the Commission with developing an annual rolling program of cyber exercises. One concrete example aimed at testing the EU's crisis management procedures is ENISA's biennial Cyber Europe series, which has simulated large-scale cyber incidents and crises affecting critical infrastructure in Europe since 2010, with its eighth edition having taken place in June 2026.[117] This pan-European exercise brings together national cyber security agencies, a number of EU agencies, bodies and networks, and experts covering a range of areas from incident response to decision-making.[118]

— Support for the integrity and availability of critical Internet infrastructure

The EU also contributes to the implementation of norm g by taking measures to protect core protocols and supporting infrastructure to ensure the functionality and integrity of the Internet worldwide. In the 2020 EU Cybersecurity Strategy, the European

116 Art. 19(3) CER Directive.

117 See further ENISA (n.d.): Cyber Europe. Cyber Europe was also mentioned by the UK as one of its activities for implementing norm G, United Kingdom Foreign & Commonwealth Office (2019): Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015.

118 ENISA (2024): Cyber Europe 2024 - After Action Report.

Commission, inter alia, envisaged to develop a contingency plan, supported by EU funding, for dealing with extreme scenarios affecting the integrity and availability of the global Domain Name System (DNS) root system. To that end, it intended to work with ENISA, the Member States, the two EU DNS root server operators, Netnod and RIPE NCC, and the multi-stakeholder community, to assess the role of these operators in guaranteeing that the Internet remains globally accessible in all circumstances.

Responding to requests for assistance (Norm H)

States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions, and/or partnerships in place to respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts?

Examples of activities that support the objective of responding to requests for assistance in cases of malicious ICT acts:

- Establishing a process for mutual operational assistance, including mutual legal assistance;
- Introducing a mechanism to cover costs related to the deployment of expert teams in the context of assistance operations;
- Developing a framework enabling the involvement of the private sector in supporting responses to assistance requests;
- Establishing a framework for coordinated response to large-scale cyber incidents and crises; and
- Conducting regular cyber exercises to strengthen mutual assistance capabilities.

The following sections provide an overview of the EU's approach to implementing these activities.

— Establishment of a regional framework for mutual operational assistance between EU Member States, including mutual legal assistance

The 2022 EU Policy on Cyber Defence recognizes that significant cybersecurity incidents are often too disruptive for a single or several affected Member States to handle alone.

In such cases, mutual assistance and solidarity[119] represent an important feature of the EU's cooperation mechanisms. In addition, in stipulating the tasks of national CSIRTs in EU Member States, the NIS2 Directive explicitly lists "providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request" as part of their mandate.[120]

Moreover, in the framework of the Permanent Structured Cooperation in Security and Defence Policy, PESCO, EU Member States have been collaborating through the project Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) since 2018.[121] The goal of the CRRT project is the development of a cyber capability that can be deployed "as a response to cyber incidents and crises as well as a preventative measure [...] in time of need."[122] In addition to Member States, beneficiaries can also be EU institutions, CSDP missions and operations, as well as EU partner countries.[123] The role of such teams is to provide tailored and targeted short-term assistance upon request and depending on the specific needs in each case.

Response through the justice system is another important part of the EU's assistance offer. The European Cybercrime Centre hosts the Joint Cybercrime Action Taskforce (J-CAT). Its mission is to drive intelligence-led, coordinated action against key cybercrime threats through cross-border investigations and operations by its partners.[124] J-CAT is open to occasional contributions from non-participating countries and non-law enforcement partners on a case-by-case basis. This can also be done within the framework of a J-CAT Attachment Scheme, which provides for a temporary attachment to collaborate on a cybercrime case with links to at least two current J-CAT member countries. Some of its past achievements include arresting 150 individuals for drug sales in dark web,[125] 12 targeted for involvement in ransomware operations against critical infrastructure,[126] and taking down the Imminent Monitor Remote Access Trojan (IM-RAT) used across 124 countries.[127]

---

119 Art. 42(7) of the Treaty of the European Union (TEU), known as the mutual assistance clause, stipulates the following: "If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter." Art. 222 of the Treaty on the Functioning of the European Union (TFEU), known as the "solidarity clause," stipulates that "should a Member State be the object of a terrorist attack or the victim of a natural or man-made disaster, the other Member States shall assist it at the request of its political authorities. To that end, the Member States shall coordinate between themselves in the Council."

120 Art. 11(3) NIS2 Directive.

121 See further PESCO (2025): (LT) Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) and Council of the EU (2019): Cyber Rapid Response Teams and Mutual Assistance in Cyber Security. The CRRT PESCO project is coordinated by Lithuania, with Belgium, Croatia, Estonia, Lithuania, the Netherlands, Poland, Romania, Slovenia, Denmark, Austria, Latvia, and Italy as participating Member States. Finland, France, Greece, and Spain are observers.

122 Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (n.d.): About.

123 Past deployments of CRRTs include the EUTM mission in Mozambique and support for the cybersecurity of European Parliamentary elections in Lithuania, PESCO (2025): (LT) Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT). CRRTs also form part of the Union's political commitments. In the Joint Declaration following the first Republic of Moldova–EU Summit in 2025, the EU reaffirms its support, stating that it "stands ready to continue supporting Moldova's digital transformation and cybersecurity, including through Cyber Rapid Response Teams," Council of the EU (2025): EU-Moldova Summit (Chisinau, 4 July 2025) - Joint Statement.

124 Europol (n.d.): Joint Cybercrime Action Taskforce (J-CAT).

125 Europol (2021): 150 arrested in dark web drug bust as police seize €26 million.

126 Europol (2021): 12 targeted for involvement in ransomware attacks against critical infrastructure.

127 Europol (2019): International crackdown on RAT spyware, which takes total control of victims' PCs.

— Introduction of a regional mechanism to cover costs related to the deployment of expert teams in the context of Member State-to-Member State mutual assistance operations

The EU Cyber Solidarity Act puts in place new procedures and cooperation modalities among EU Member States, such as a comprehensive Cybersecurity Emergency Mechanism to improve the EU's cyber resilience.[128] As part of the Cyber Solidarity Act's Emergency Mechanism, the Regulation also seeks to enhance "technical assistance from one Member State to another Member State affected by a significant cybersecurity incident or a large-scale cybersecurity incident."[129] In this respect, it provides for the possibility of a supporting Member State to request a grant, funded by the Digital Europe Programme, that covers costs related to the deployment of its experts in another Member State, such as travel, accommodation, and daily allowances.

— Development of a framework enabling the involvement of the private sector in supporting responses to assistance requests

In the framework of its Cybersecurity Emergency Mechanism, the Cyber Solidarity Act also provides for the establishment of a so-called EU Cybersecurity Reserve, a validated pool of incident response services from private service providers ("trusted providers"), which can assist Member States cyber crisis management authorities and national CSIRTs or CERT-EU in addressing significant or large-scale cybersecurity incidents.[130] The Regulation stipulates how these users can "request services […] to support response to and initiate recovery from significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents."[131] The costs for the provision of these services are covered by the Digital Europe Program. ENISA is responsible for administering and operationalizing the EU Cybersecurity Reserve.[132] In addition to EU Member States and CERT-EU as users of the Reserve, the Regulation also provides for the possibility that services may be requested by associated third countries under specific circumstances. As of July 2026, the EU has granted Moldova and Ukraine access to these services as well.[133]

128 European Commission (n.d.): EU Cyber Solidarity Act.

129 Art. 18 CSOA.

130 See also ENISA (n.d.): EU Cybersecurity Reserve.

131 Art. 15 CSOA.

132 ENISA (2025): ENISA to operate the EU Cybersecurity Reserve with EUR 36 million.

133 Council Implementing Decision 2025/1458 authorising support from the EU Cybersecurity Reserve for Moldova and Council Implementing Decision 2026/1354 authorising the provision of support from the EU Cybersecurity Reserve to Ukraine.

— Establishment of a regional framework for coordinated response to large-scale cyber incidents and crises

The EU has put in place an extensive framework for assisting its member states and allies who are victims of malicious cyber activities. The EU's Blueprint for cyber crisis management applies to cybersecurity incidents which cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or EU institutions with such a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level.

— Conduct of regular cyber exercises to strengthen mutual assistance capabilities

Exercises are a critical aspect of strengthening cooperation modalities to better meet requests for assistance. The EU's 2022 Strategic Compass for Security and Defence commits to regular cyber exercises starting from 2022, with the objective of further strengthening the EU's mutual assistance in the event of armed aggression. Further relevant exercises at EU level include Cyber Europe (see further section on norm g) or CySOPex and BlueOLEx in the area of crisis management.[134]

Ensuring supply chain security (Norm I)

States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions, and/or partnerships in place to ensure the integrity of the supply chain and the safety and security of ICT products throughout their lifecycle?
- Q2: Does the EU have legislation, policies, institutions and/or partnerships in place to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions?

134 See further, for example, ENISA (2025): BlueOLEx 2025: Testing the Capabilities of EU Crisis Management Executives.

Examples of activities that support the objective of ensuring ICT supply chain security:

- Introducing a legal framework requiring specific entities to implement supply chain risk management measures;
- Creating a cybersecurity certification framework for ICT products;
- Adopting cybersecurity requirements for products with digital elements through a product safety regulatory framework;
- Expanding product liability frameworks to ICT products;
- Integrating supply-chain security provisions within cybersecurity strategies;
- Conducting and coordinating security risk assessments for critical ICT supply chains;
- Introducing measures to mitigate cybersecurity risks associated with 5G networks;
- Articulating an understanding of key ICT supply chain concepts, risk scenarios, and mitigation recommendations; and
- Issuing advisories, guidance, and reports on supply chain security.

The following sections provide an overview of the EU's approach to implementing these activities.[135]

— Introduction of a legal framework requiring specific entities to implement supply chain risk management measures

Through the NIS2 Directive, the EU has established several measures for the essential and important entities within its scope to strengthen supply chain security. These entities must implement appropriate and proportionate technical, operational, and organizational measures to manage risks to their network and information systems, comprising "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers" as a minimum requirement.[136] In June 2025, ENISA also published technical implementation guidance for the NIS2 Directive, that also includes a dedicated section on supply chain security, that specifically highlights putting in place a supply chain security policy and a directory of suppliers and service providers.[137]

135 For a general overview of measures that governments can take to implement norm I, see also Alexandra Paulus and Christina Rupp (2023): Government's Role in Increasing Software Supply Chain Security: A Toolbox for Policy Makers. Stiftung Neue Verantwortung.

136 Art. 21(2), point (d) NIS2 Directive.

137 ENISA (2025): Technical Implementation Guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures.

— Creation of a cybersecurity certification framework for ICT products

The EU's Cybersecurity Act (CSA) sets the foundations for an EU-wide cybersecurity certification framework for ICT products to enable the creation of tailored and risk-based EU certification schemes.[138] The certification framework provides EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. In 2024, the EU approved the first Implementing Regulation on the adoption of a European Common Criteria-based cybersecurity certification scheme based on the international standard Common Criteria which was already used to issue certificates in Europe for almost 30 years. This voluntary scheme applies across the EU to certify the cybersecurity of ICT products in their lifecycle. The scheme applies, among others, to biometric systems, firewalls (both hardware and software), detection and response platforms, routers, encrypted storages, databases, and smart cards and secure elements included in passports or other documents of daily use.

These regulatory efforts are supported through a specific framework of institutions and bodies. The European Cybersecurity Certification Group (ECCG) was established in 2019 to help ensure the consistent implementation and application of the CSA. It is composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. The ECCG supports the preparation of the candidate certificate scheme and the general implementation of the certification framework.[139] In addition, a Stakeholder Cybersecurity Certification Group (SCCG) is responsible for advising the Commission and ENISA on strategic issues regarding cybersecurity certification.[140]

— Adoption of cybersecurity requirements for products with digital elements through a product safety regulatory framework

The EU's efforts to enhance ICT supply chain security have been further strengthened through the Regulation on horizontal cybersecurity requirements for products with digital elements, also known as the Cyber Resilience Act (CRA). The CRA puts in place rules to ensure more secure hardware and software products on the EU market to guarantee that manufacturers, among other addressees, improve the security of products with digital elements throughout the whole life cycle. Measures to that end include the requirement

138 See also European Commission (2026): Report on the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework and ENISA (n.d.): Dedicated Website on EU Cybersecurity Certification.
139 European Commission (n.d.): The European Cybersecurity Certification Group.
140 European Commission (n.d.): Stakeholder Cybersecurity Certification Group.

for manufacturers to "draw […] up a software bill of materials[141] in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products"[142] (see further also the section on the EU's implementation of norm j). The CRA also strives for more transparency on the market, allowing users to take cybersecurity into account when selecting and using products with digital elements.

— Expansion of product liability frameworks to ICT products

In addition to product safety measures, the EU also contributes to strengthening supply chain security through its product liability framework. The 2024 revision of the EU's Product Liability Directive enables victims of defective products to bring claims against economic operators, which can in turn incentivize stronger security practices across supply chains. The Directive's revision now explicitly also includes software, which was previously difficult to cover due to physicality and tangibility requirements, thereby, inter alia, bringing software manufacturers within its scope.[143]

— Integration of supply-chain security provisions within EU Member States' cybersecurity strategies

Under the NIS2 Directive, EU Member States are required, as part of their national cybersecurity strategies, to adopt policies "addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services."[144]

— Coordination of security risk assessments for critical ICT supply chains

At the Union level, the NIS2 Directive provides for the development of coordinated security risk assessments of critical ICT supply chains,[145] to be carried out by the NIS Cooperation Group in cooperation with the European Commission and ENISA, to "identify measures, mitigation plans and best practices to counter critical dependencies, potential single points of failure, threats, vulnerabilities and other risks associated with the supply chain."[146] These assessments should take into account both technical and

141 A software bill of materials (SBOM) is "a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements" (Art. 3, point (39) CRA).

142 Annex I Part II (1) CRA.

143 See further, for example, Christina Kiefer and Laure Herlitz (2025): Liability for software under the new European Product Liability Directive, International Bar Association, Lena Niehoff, David Hilger, and Katie Chandler (2025): A new era for product liability in the EU, Taylor Wessing and Alexandra Paulus (2026): Cybersecurity Needs Secure Software, German Institute for International and Security Affairs. Importantly, the EU's Product Liability Directive does not apply to free and open-source software developed or supplied outside the course of a commercial activity. Paulus also points three important limitations of the Product Liability's Directive when applied to the area of software security: "only natural persons may bring claims, only software used exclusively for private purposes qualifies, and claims arise only in cases of personal injury, property damage, or data damage."

144 Art. 7(2), point (a) NIS2 Directive.

145 Art. 22 NIS2 Directive.

non-technical risk factors relevant to the supply chains studied. In January 2026, the NIS Cooperation Group published two coordinated risk assessments on connected and automated vehicles as well as detection equipment.[147]

— Introduction of regional measures to mitigate cybersecurity risks associated with 5G networks

Building upon a coordinated risk assessment of the cybersecurity of 5G networks and Council conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G,[148] the EU's NIS Cooperation Group adopted a 5G toolbox in January 2020. The objectives of the EU's 5G Cybersecurity Toolbox are identifying a possible common set of measures to mitigate the main cybersecurity risks of 5G networks to ultimately create a robust framework of measures with a view to ensure an adequate level of cybersecurity of 5G networks across the EU and coordinated approaches among Member States.[149] This includes "strengthening own 5G capabilities to avoid dependencies and to foster a sustainable and diverse supply chain." The Cybersecurity 5G Toolbox outlines a catalog of 19 either strategic or technical mitigation measures, which the toolbox complements with ten supporting actions. Strategic measures, inter alia, include the expansion of national regulatory powers and the strengthening of domestic resilience. On a technical level, the Toolbox stipulates concrete measures that involve, for example, the "application of baseline security requirements," an "evaluati[on of] the implementation of security measures in existing 5G standards," and the enhancement of "software integrity, update and patch management." The second Progress report on the implementation of the EU 5G Toolbox by the NIS Cooperation Group provides an overview of the challenges and practices across the EU.[150]

— Articulation of a regional understanding of key ICT supply chain concepts, risk scenarios, and mitigation recommendations

In January 2026, the NIS Cooperation Group published an advisory ICT Supply Chain Security Toolbox, which EU Member States invited the Group to develop in October 2022 through their Council conclusions on ICT supply chain security.[151] The Toolbox

146 Recital (90) NIS2 Directive.

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

148 European Commission (2019): EU-wide coordinated risk assessment of 5G networks security and Council of the EU (2019): Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G.

149 European Commission (2020): Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures.

150 European Commission (2023): Communication from the Commission: Implementation of the 5G cybersecurity Toolbox.

151 In terms of further instruments to strengthen supply chain security, EU Member States further note in their 2022 Council conclusions that the "EU's Foreign Direct Investment Screening mechanism […] could also be applied as a useful tool for safeguarding security and resilience of the ICT supply chain" and refer to public procurement as a relevant instrument by focusing on the "cybersecurity practices of tenderers and their subcontractors."

seeks to "define[…] key concepts related to the ICT supply chain, identif[y] potential risk scenarios affecting ICT supply chains within the Union, and provide recommendations to address and mitigate these risks," thereby also providing a framework for carrying out coordinated risk assessments under the NIS2 Directive. Building on the definition of supply chain incidents – that the document refers to as an "incident […] in which something that should be delivered (e.g. a new software feature or antivirus signature in an update) is not delivered, or should not be delivered (e.g. malware concealed in a software update or a limiting configuration in a component) is delivered" – and four main categories of threats – namely malicious actions, system failures, human error, and natural phenomena or external events – the toolbox develops eleven detailed risk scenarios. These scenarios analyze, for each case, factors such as the type of incident, the threat source, involved supply chain entities, user phases affected, threat actors, vulnerabilities, and resulting impacts. Its annex provides three detailed lists of examples of threats, vulnerabilities, and impacts relevant to ICT supply chains.

— Issuance of advisories, guidance, and reports on supply chain security

As part of its mandate, ENISA is also issuing advisories and publications that address supply chain security. For instance, ENISA published a dedicated threat landscape report on supply chain attacks, provided guidance detailing good practices for supply chain security, or issued an advisory advising on the secure use of package managers in software development.[152]

Reporting ICT vulnerabilities (Norm J)

States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions and/or partnerships in place to encourage responsible reporting of ICT vulnerabilities and mitigation sharing?

Examples of activities that support the objective of responsibly reporting ICT vulnerabilities and mitigation-sharing:

152 ENISA (2021): Threat Landscape for Supply Chain Attacks, ENISA (2023): Good Practices for Supply Chain Cybersecurity and ENISA (2026): ENISA Technical Advisory for Secure Use of Package Managers.

- Integrating vulnerability disclosure provisions within cybersecurity strategies;
- Designating CSIRTs as coordinated vulnerability disclosure (CVD) coordinators;
- Establishing regional information-sharing mechanisms and collaboration among CVD coordinators;
- Introducing a legal framework requiring specific entities to implement vulnerability disclosure and handling measures;
- Establishing a legal framework addressing vulnerability handling and reporting requirements for products with digital elements;
- Developing and supporting vulnerability management initiatives;
- Issuing advisories, guidance, and reports on vulnerability disclosure policies and vulnerability mitigation.

The following sections provide an overview of the EU's approach to implementing these activities.[153]

— Integration of vulnerability disclosure provisions within EU Member States' cybersecurity strategies

Under the NIS2 Directive, EU Member States are required, as part of their national cybersecurity strategies, to adopt policies on "managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure."[154] As part of its work on providing an overview over national cybersecurity strategies, ENISA maintains an overview of how Member States have put this commitment in place.[155]

— Designation of national and EU CSIRTs as coordinated vulnerability disclosure coordinators

The EU addresses Coordinated Vulnerability Disclosure (CVD) through regulatory and institutional means. According to the NIS2 Directive, each Member State must designate one of its CSIRTs as a coordinator for the purposes of CVD. The main task of such coordinator is to act as a "trusted intermediary," including facilitating, where necessary, the interaction between the organization or a person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services. The CVD coordinator shall ensure that diligent follow-up action is carried out with regard to

153 For a general overview of measures that governments can take to implement norm j, see also Sven Herpig (2024): Vulnerability Disclosure: Guiding Governments from Norm to Action: How to Implement Norm J of the United Nations Norms of Responsible State Behaviour in Cyberspace, interface.

154 Art. 7(2), point (c) NIS2 Directive. See further also Commission Implementing Regulation 2024/2690 laying down rules for the application of Directive 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

155 ENISA (n.d.): CVD Policy.

the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. In addition, ENISA has worked on developing mechanisms to encourage the use of CVD practices and supported Member State CSIRTs in the adoption and development of CVD policies at the national level. The EUIBAs Regulation designates CERT-EU as an equivalent CVD coordinator for the Union entities.

— Establishment of regional information-sharing mechanisms and collaboration among national coordinated vulnerability disclosure coordinators

The NIS2 Directive also provides for the cooperation of national CVD coordinators with their counterparts in the Union. Specifically, if, upon reporting of a vulnerability, they determine that the vulnerability "could have a significant impact on entities in more than one Member State," national CVD coordinators shall interact with their counterparts in other EU Member States through the framework of the CSIRTs Network. This is of relevance because the CSIRTs Networks tasks comprise "exchang[ing] relevant information about incidents, near misses, cyber threats, risks and vulnerabilities" and "at the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities."[156] The NIS Cooperation Group is, inter alia, responsible for providing guidance on developing and implementing national CVD policies.

— Introduction of a legal framework requiring specific entities to implement vulnerability disclosure and handling measures

Through the NIS2 Directive, the EU has established several measures for the essential and important entities within its scope to incorporate vulnerability disclosure. These entities must implement appropriate and proportionate technical, operational, and organizational measures to manage risks to their network and information systems, comprising "security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure" as a minimum requirement.[157] In June 2025, ENISA also published technical implementation guidance for the NIS2 Directive, that also includes a dedicated section on vulnerability handling and disclosure.[158]

156 Art. 15(3) NIS2 Directive.
157 Art. 21(2), point (e) NIS2 Directive.
158 ENISA (2025): Technical Implementation Guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures.

— Establishment of a legal framework addressing vulnerabil-ity handling and reporting requirements for products with digi-tal elements

Furthermore, the EU has addressed vulnerability management – including their disclosure – with vulnerability handling requirements provided for in the Cyber Resilience Act. For instance, the regulation requires that "manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources."[159] This includes, inter alia, systematically documenting relevant vulnerabilities that manufacturers become aware of, identifying and documenting vulnerabilities and software components, and ensuring that vulnerabilities are fixed or mitigated in a timely manner. The CRA also introduces reporting obligations, requiring manufacturers to notify any actively exploited vulnerability to the respective national authority and ENISA as soon as they become aware of it. In addition, the CRA provides that importers and distributors of products with digital elements must promptly inform manufacturers if they become aware of vulnerabilities in those products. The regulation further imposes obligations on so-called open-source software stewards, requiring them to establish and document a cybersecurity policy that specifically addresses vulnerability handling, contributes to fostering voluntary reporting to national authorities or ENISA, and promotes information-sharing on discovered vulnerabilities within the open-source community.

— Development and support for vulnerability management initiatives

The NIS2 Directive also mandates ENISA to develop and maintain a European Vulnerability Database (EUVD) serving as a repository of all reported vulnerabilities.[160] The Database should include "information describing the vulnerability; the affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited; and the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated."[161]

ENISA launched the EUVD in May 2025.[162] Since January 2024, ENISA has acted as a Numbering Authority for the Common Vulnerabilities and Exposures (CVE) program (CNA)

159 European Commission (2022): Cyber Resilience Act.
160 ENISA (2024): Another step forward towards responsible vulnerability disclosure in Europe.
161 Art. 12(2) NIS2 Directive.

authorized to assign CVE Identifiers (CVE IDs) and publish CVE Records for vulnerabilities discovered by or reported to EU CSIRTs. In November 2025, ENISA has elevated its role in the CVE program and became a CVE Program Root which, inter alia, entails "taking on additional responsibilities including the identification, onboarding, and support to other CNAs within its scope."[163]

— Issuance of advisories, guidance, and reports on vulnerability disclosure policies and vulnerability mitigation

At the EU level, the NIS Cooperation Group, ENISA, and CERT-EU are involved in the issuance of advisories, guidance, and reports on vulnerability disclosure policies and vulnerability. In 2023, the NIS Cooperation Group adopted guidelines on implementing national CVD policies. The guidelines address the roles involved in implementing a CVD policy, the legal challenges states may encounter when establishing such a framework, the key elements such mechanisms should include, and recommendations to support their adoption by states.[164] The same year, ENISA published a report on developing national vulnerability programs.[165] A year earlier, in 2022, ENISA issued a report on the CVD landscape in the EU.[166] The report provides an overview of the CVD practices in all EU Member States, identifies good practices, and offers concrete recommendations for addressing legal, economic, political and operational challenges associated with CVD processes. ENISA's recommendations encompass defining the role of ethical hackers in relevant national laws to establish a framework for ethical security research around vulnerabilities and developing incentives for security researchers to actively participate in CVD research. Back in 2022, the report found that Belgium, France, Lithuania and the Netherlands undertook CVD policy work and have implemented policy requirements while other Member States were at different stages or have not implemented a CVD policy yet. ENISA and CERT-EU are also active in issuing advisories and statements that include remediation recommendations, addressing, for example, the exploitation of specific vulnerabilities, how to identify them, and ways to mitigate their potential impact.[167]

162 ENISA (n.d.): European Vulnerability Database.

163 ENISA (2025): Stepping up our role in Vulnerability Management: ENISA Becomes CVE Root and ENISA (2026): New CVE Numbering Authorities Under ENISA Root.

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

165 ENISA (2023): Developing National Vulnerabilities Programmes. Another example of a relevant ENISA report is ENISA (2023): Cybersecurity Investment: Spotlight on Vulnerability Management.

166 ENISA (2022): Coordinated Vulnerability Disclosure Policies in the EU.

167 See, for example, ENISA (2024): Joint Statement on Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities, CERT-EU (2024): Security Advisory 2024-004 – Critical Vulnerabilities in Ivanti Connect Secure, ENISA (2025): Joint Statement on SharePoint vulnerabilities - Assessment and advice on recovery and mitigating actions, ENISA (2021): Joint Statement on Log4Shell and ENISA (n.d.): CNW/advisories. GitHub.

Not harming emergency response teams (Norm K)

States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (CERTs/CSIRTs) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Key question(s) for assessing the EU's norm implementation:

- Q1: Does the EU have legislation, policies, institutions, and/or partnerships in place to address the use of ICT that intentionally harms the information systems of the authorized CERTs/CSIRTs of another State?
- Q2: Does the EU have rules that prohibit using CERTs/CSIRTs to engage in malicious international activity?

Examples of activities that support the objective of not harming foreign CERTs/ CSIRTs:

- Establishing a legal framework defining the roles and responsibilities of CSIRTs;
- Facilitating cooperation among CSIRTs and participation in CSIRT networks; and
- Publishing and maintaining a list of declared national CSIRTs at a regional/international level.

Given that EU Member States have full competence over their national security, the EU's role in the implementation of the UN cyber norms of a prohibitive nature is rather limited. Nonetheless, the EU has taken certain measures that provide an overall framework for the role that CERTs/CSIRTs play within its cyber ecosystem. The following sections provide an overview of the EU's approach to implementing these activities.

— Establishment of a legal framework defining the roles and responsibilities of national CSIRTs and CERT-EU

Although the EU has introduced measures concerning the establishment of CSIRTs, there are no legal EU-wide rules concerning the prohibition of malicious activity against other CERTs or CSIRTs. The second component of the norm – setting out the expectation that states should not use authorized emergency response teams to engage in malicious international activity – is more directly reflected in EU legislation through the strictly bounded mandates of national CSIRTs and CERT-EU, which restrict the intrusive scope of these entities.

Under the NIS2 Directive, national CSIRTs of EU Member States should, inter alia, have the following tasks in relation to essential and important entities:

- "monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance of essential and important entities regarding real-time or near real-time monitoring of their network and information systems;
- providing early warnings, alerts, announcements and dissemination of information […] on cyber threats, vulnerabilities and incidents, if possible in near real-time;
- responding to incidents and providing assistance […];
- collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;
- providing, upon […] request […], a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;
- participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network […]."[168]

The EUIBAs Regulation stipulates the mandate of CERT-EU and its tasks, including "offer[ing] standard CSIRT services for Union entities," "coordinat[ing] the management of major incidents," and "provid[ing], upon the request of a Union entity, proactive non-intrusive scanning of publicly accessible network and information systems of that Union entity."[169]

— Facilitation of cooperation among CSIRTs and participation in CSIRT networks

The NIS2 Directive explicitly mentions that CSIRTs may establish cooperation with such teams in other countries and that EU Member States should ensure that exchange of information between these bodies is effective, efficient and secure. The CSIRTs may also cooperate for the purpose of providing cybersecurity assistance. CERT-EU is also a member of the Forum for Incident Response and Security Teams (FIRST).[170] While not explicitly prohibiting malicious conduct, such arrangements can create routine coordination mechanisms and foster personal contacts that establish clear mutual expectations of non-malicious activity between the CSIRTs and authorities involved.

— Publication and maintenance of a list of declared national CSIRTs in the EU

On its website, the CSIRTs Network maintains a list of declared national CSIRTs in the EU. This contributes to the clear identification and recognition of authorized CSIRTs of EU Member States, which should thus be considered off limits as targets. In doing so, the

168 Art. 11 NIS2 Directive.
169 Art. 13(3) Regulation 2023/2841.
170 Forum of Incident Response and Security Teams (n.d.): FIRST Teams.

list reduces potential ambiguity regarding which entities qualify as protected CSIRTs under this specific norm.[171]

External Implementation: How the EU Supports Norms Implementation Through Capacity Building

Despite the growing political fragmentation within the UN cyber-related processes, states have consistently agreed on the need to accelerate international assistance to support the implementation of the framework of responsible state behavior in cyberspace.[172] The UN GGE 2021 report identified a set of concrete goals for such capacity building, including policy and strategy development, legislation and regulation, incident response capacities, protection of critical infrastructure, cybercrime and criminal justice capacities, confidence-building and cooperation, public awareness and education, and broader support for resilience and secure digital development.[173]

Nonetheless, while the link between capacity building and norms implementation is, in theory, widely recognized and reflected in policy documents and UN discussions, the connection remains largely indirect in practice.[174] Often, states strengthen laws on cybercrime, establish reporting obligations for critical infrastructure operators, improve vulnerability handling procedures, or create crisis coordination mechanisms without ever framing these efforts as part of the UN norms agenda. Also, in 2022, EU Member States "emphasi[zed] the need to better connect the EU's cyber capacity building strategy with the UN norms of responsible State behaviour in cyberspace."[175]

Still, most capacity building initiatives are instrumental for norms implementation because the UN norms are not self-executing. They can shape state behavior only when states possess the institutions, legal frameworks, operational procedures and human expertise necessary to implement them in practice. Capacity building is therefore not just

171 CSIRTs Network (n.d.): CSIRTs Network Members. Declaring a list of (national) CSIRTs is also listed in the ASEAN Norms Implementation Checklist and a preceding UNIDIR paper mapping relevant implementation activities, ASEAN (2025): ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace and Samuele Dominioni and Giacomo Persi Paoli (2023): Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities. UNIDIR.

172 Nayia Barmpaliou and Patryk Pawlak (2025) Between ambition and pragmatism: The future of cyber capacity-building in a fragmented world, European Union Institute for Security Studies.

173 United Nations General Assembly (2021): Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135). The EU's cyber capacity-building practice is increasingly reflecting the same priorities. In that regard, the EU's 2023 Operational Guidance on external cyber capacity building identifies five principal policy pillars for EU action: national strategic cyber frameworks, criminal justice in cyberspace, cyber crisis prevention and management, cybersecurity education and culture, and cyber diplomacy, European Commission (2023) Operational Guidance: The EU's international cooperation on cyber capacity building.

174 See also Christina Rupp (2025): Signals in the Noise: Building Governmental Capabilities to Detect Cybersecurity Threats, interface.

175 Council of the European Union (2022): Council conclusions on the development of the European Union's cyber posture, 9364/22.

a supporting activity around norms implementation. In many cases, it is one of the principal ways implementation actually happens and can function as a bridge between international agreement and domestic practice.[176] As a result, states – and regions – can contribute to implementation not only by adopting or adapting their domestic and regional frameworks to establish the prerequisites for putting these behavioral expectations into practice, but also by supporting others in developing and enhancing the capacity to do the same.[177]

This chapter analyzes how the EU does the latter by exploring ways in which it supports the implementation of the UN cyber norms through capacity building in partner countries and regions. This chapter uses the capacity building goals identified by the UN GGE as an organizing framework to show how each capacity area matters for implementing the UN norms and to illustrate each capacity area with examples of relevant EU projects or initiatives.[178] The examples included for the EU's external implementation pathway are intended to illustrate existing efforts rather than provide an exhaustive overview, especially given the complexity and breadth of the cyber capacity building landscape.

Policy and strategy development

Policy and strategy development is fundamental for norms implementation because the UN framework requires states to translate broad international expectations into national priorities, institutional mandates and implementation pathways. Without national strategies and policy frameworks, implementing the norms on cooperation, due diligence, assistance, critical infrastructure protection or human rights respecting cybersecurity remains fragmented and dependent on ad hoc political choices rather than sustained governance. For example, in its guidance on norm a, the 2021 UN GGE encouraged states to put in place or strengthen relevant policy, legislation, review processes, crisis-management mechanisms and whole-of-government partnerships in order to support cooperation and stability in the use of ICTs. Also in its discussion of other norms, the report repeatedly linked implementation to national structures, ICT-related policies, and coordination mechanisms. Policies and strategies can thus help states identify priorities, assign roles, sequence reforms and create a strategic framework through which individual norms can be implemented coherently rather than in isolation.

176 For that reason, the ASEAN Norms Implementation Checklist, for example, also specifically includes suggested capacity-building activities that enable states to put in place the enumerated implementation measures, ASEAN (2025): ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace. See also Samuele Dominioni and Giacomo Persi Paoli (2023): Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, UNIDIR.

177 In applying the norm life cycle concept to the area of cyberspace, Finnemore and Hollis also explicitly examine cyber capacity building as an instrument to enhance the socialization of norms, Martha Finnemore and Duncan B. Hollis (2017): Constructing Norms for Global Cybersecurity, American Journal of International Law.

178 For a full mapping of EU-funded cyber capacity building projects and initiatives, see EU CyberNet (n.d.) CCB projects mapping.

The EU has supported this capacity area through projects such as **EU CyberNet** which provides on-demand support for partner countries in policy and strategy development and operates as a flexible platform connecting EU expertise with the needs of third countries.

Legislation and regulation

As the implementation activities identified in Chapter 4 underscore, implementation requires domestic rules and efforts that specify institutional responsibilities, investigative powers, resilience obligations and safeguards to move from political endorsement to practical operationalization. Implementing the norms on preventing misuse of ICTs, prosecuting cybercrime, protecting critical infrastructure, responding to requests for assistance, reporting vulnerabilities or respecting privacy and human rights thus significantly benefits from legislation or regulation that clarifies duties, powers, safeguards and accountability.[179] Legal capacity is thus not peripheral to norm implementation but represents one of its principal enabling conditions.

There are several EU initiatives aimed at accelerating these capacities: Through the **ESIWA+** project in Asia and the Indo-Pacific, the EU has, for example, supported Malaysia's National Cyber Security Agency during the legislative process leading to adoption of the Cyber Security Act in 2024. Through **CyberEAST+**, the EU supports partner countries in carrying out legislative reforms and strategy development in the area of cybercrime and broader cyber governance. This also includes support for the development and implementation of policies aligned with the European Union legislation in the field of cybersecurity, particularly the NIS2 Directive. The **Cyber Balkans** project supported the Western Balkans in building stronger cybersecurity governance and resilience aligned with EU standards and international good practices.

Incident response capacities

States rely on incident response capacities, including CERTs/CSIRTs, to implement the UN norms, as many of its expectations require them to detect,[180] analyze, mitigate, and recover from malicious ICT activity. A state cannot meaningfully implement norms on due diligence, attribution, cooperation, requests for assistance, critical infrastructure protection or vulnerability handling if it lacks a competent technical body capable of receiving reports, analyzing incidents and coordinating responses.[181]

179 The 2021 GGE report reflected this directly. It noted, for example, that states can establish or strengthen legislative frameworks to investigate and resolve incidents, that observance of the norm on criminal and terrorist use of ICTs implies national legislation and structures facilitating cross-border cooperation, and that implementation of the norm on critical infrastructure may require relevant policy and legislative measures with review and oversight, United Nations General Assembly (2021): Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

180 On the nexus between detection capabilities and norms implementation, see also Christina Rupp (2025): Signals in the Noise: Building Governmental Capabilities to Detect Cybersecurity Threats, interface.

The **Cybersecurity Rapid Response 2.0** project contributes to strengthening the operational capacities of Security Operations Centers and CSIRTs in Albania, Montenegro, and North Macedonia. Also in this capacity area, **EU CyberNet** is active by supporting CSIRT capability-development and offering expertise on incident response and cyber governance, especially through the work conducted by the Latin America and Caribbean Cyber Competence Centre (LAC4).

Cyber crisis prevention and management

Cyber crisis prevention and management capacities are essential for implementing the UN cyber norms because several of them become most relevant during high-impact incidents: the obligation to consider all relevant information, the expectation to cooperate, the commitment to protect critical infrastructure and the norm on responding to requests for assistance all depend on having crisis-management structures, playbooks and chains of communication already in place. The past UN processes have explicitly encouraged mechanisms for crisis and incident management under norm a and underlined the importance of consultation, notification, acknowledgement, and assistance procedures under norms b, c and h.

Cyber crisis prevention and management have become part of the EU's engagement with international partners through existing projects, even when it was not an initial primary objective. For instance, the EU funded **International Cybersecurity Command and Staff Exercises** in Moldova with the participation of Ukraine. The key objectives of the practical sessions included, among others, identifying areas for improvement in cross-border crisis management and strengthening trust and operational alignment among partners.

Critical infrastructure protection

One of the key areas for norms-related capacity building – and strengthening cyber resilience more broadly – is the protection of critical infrastructure. Enhancing these capacities enables states to give effect to several norms simultaneously: those relating to non-damage, protection, and assistance related to critical infrastructure as well as those pertaining to due diligence, supply chain security and vulnerability disclosure. At the same time, these norms are among the most operationally demanding in the framework. They require states to identify critical sectors, assess risks, establish protective measures, coordinate with infrastructure owners and operators, and prepare to provide or request assistance when incidents occur.

181 The 2021 GGE report repeatedly emphasized this point. It recommended cooperation among national CERTs and CSIRTs, ICT authorities and the diplomatic community, encouraged strengthening mechanisms for crisis and incident management, and highlighted the value of national structures and processes to assess the severity and replicability of ICT incidents, United Nations General Assembly (2021): Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

The **EU's Eastern Partnership Cybersecurity Initiative** aims at strengthening national cybersecurity governance and legal framework across the Eastern Partnership (EaP) countries in line with the NIS2 Directive, developing critical information infrastructure frameworks in the EaP countries, and increasing operational capacities for cybersecurity incident management in the EaP countries.

Cybercrime and criminal justice capacities

Addressing cybercrime and strengthening criminal justice capacities has historically been one of the most advanced cyber capacity building efforts.[182] This capacity area is particularly indispensable to the implementation of norm d, which calls on states to cooperate in exchanging information, assisting one another, prosecuting terrorist and criminal use of ICTs and implementing other cooperative measures. It is also relevant to other norms, because a state, for instance, cannot take appropriate and feasible steps against internationally wrongful acts or malicious activity emanating from its territory if it lacks investigative and prosecutorial capacities.[183] Efforts aimed at enhancing criminal justice capacities in partner countries can therefore not only be confined to supporting domestic law enforcement but also contribute to wider norms implementation by making states able to cooperate, investigate and respond lawfully.

The EU has a broad portfolio in this area. The **Global Action on Cybercrime Enhanced (GLACY-e)** project strengthens the capacity of actors within the criminal justice ecosystem to investigate and prosecute cybercrime and cooperate across borders. **CyberSEE** and **CyberEAST+** also provide assistance on legislative reforms, strategy, training of judiciary and law enforcement, public-private partnerships and international cooperation, thereby helping states build cybercrime units, evidence-handling procedures and cooperation practices that reduce impunity for malicious actors and strengthen trust among states.

International partnerships and cyber diplomacy

Given that the UN framework is built on the premise that stability in cyberspace depends on cooperation among states and engagement with other stakeholders, states need capacities to engage with other countries and build partnerships. Norm a is explicitly about cooperation to increase stability and security, while other norms benefit from consultation, notification, requests for assistance, multistakeholder exchanges and

182 Robert Collett and Nayia Barmpaliou (2021) International cyber capacity building: global trends and scenarios, European Union Institute for Security Studies and Robert Collett and Nayia Barmpaliou (2021) International cyber capacity building: global trends and scenarios - annex 3, European Union Institute for Security Studies.

183 The 2021 GGE report made this link explicit by highlighting that the observance of norm d implies national policies, legislation, structures and mechanisms that facilitate cooperation across borders on technical, law-enforcement, legal and diplomatic matters. The report also recommended protocols and procedures for collecting, handling and storing online evidence and providing timely assistance in investigations, United Nations General Assembly (2021): Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

regional platforms. Capacity building initiatives can help create the partnerships, shared understandings, and trusted channels necessary to carry out these functions.

There are several practical examples of the EU's efforts in this domain. The **Tallinn Cyber Diplomacy programme**, funded under the Global Gateway strategy, is a unique platform providing training for diplomats and cyber professionals from all over the world. The **EU Cyber Diplomacy Initiative**, EU Cyber Direct, supports the EU's capacity building efforts through multistakeholder engagement and a fellowship program. Another practical example is **EU CyberNet**, which hosts regional events, stakeholder meetings, community-building activities and a knowledge hub intended to strengthen coordination and knowledge-sharing across the EU's external cyber assistance community and partner countries.

Awareness, education and cybersecurity culture

Governmental capacities in the areas of awareness, education and cybersecurity culture are often underestimated in norm implementation debates. Yet, they are important because norms are implemented not only through laws and agencies but are linked to the behavior of users, operators, officials, researchers, and companies that make up the wider cybersecurity (policy) ecosystem. Without awareness and trained personnel, states may have institutions on paper but remain limited in sustaining secure practices, protecting infrastructure, or handling vulnerabilities.[184] Strengthening human capital and skills therefore matters for norms implementation because several norms, especially those addressing critical infrastructure protection, vulnerability disclosure, and human rights, presuppose a public sector workforce and stakeholder community able to understand and apply good practices.

Several projects mentioned in this chapter, especially **EU CyberNet** or **ESIWA+**, address the identified capacity gaps but many others include cyber-related elements of awareness raising. Moreover, broad training and awareness elements are also embedded in projects such as **CyberEAST+** and **CyberSEE**, including training for judiciary, law enforcement and public-private partnerships.

184 Without proper awareness, education and culture, the accountability of government officials is also weakened, Patryk Pawlak (2024) Accountability in Cyberspace: The Holy Grail of Cyber Stability?. EU Cyber Direct.

Takeaways

The implementation of the UN cyber norms is ultimately about one simple idea. Cyber norms only matter when they show up in everyday decisions and shape what governments actually do in the cyber domain. The EU provides an instructive case for examining how abstract UN commitments turn into concrete practices, especially because the EU pursues different implementation mechanisms concurrently, albeit to varying degrees.

The EU's experience indicates several important conclusions about that process:

1. **The EU already implements the UN cyber norms extensively and at scale across its cyber policy ecosystem**. Existing EU instruments and mechanisms – such as the NIS2 Directive, the Cyber Solidarity Act, cyber diplomacy tools, cyber capacity building initiatives, and the activities of actors like ENISA and the CSIRTs Network – contribute to the operationalization of all eleven norms. The implementation of UN cyber norms in the EU is therefore already embedded across multiple domains of governance rather than driven by a single policy area, institution, or instrument.
2. **The EU's norms implementation is an inherently dynamic and continuous process**. The EU experience demonstrates that implementation is not a single downstream step, but a prolonged process of translation, institutionalization, and revision. As digitization expands and critical sectors become more interconnected, the EU has treated many of its implementation mechanisms, especially legal instruments, not as fixed endpoints, but as tools that it has repeatedly updated to broaden coverage, clarify obligations, and address practical shortcomings identified during initial stages of implementation.
3. **The EU's implementation is driven by a number of cross-cutting enabling capabilities, rather than by isolated measures contributing only to individual norms**. These capabilities include, at a minimum, cybersecurity coordination structures and agencies, strategic cybersecurity frameworks, the establishment of national and EU CSIRTs, regulatory frameworks addressing critical infrastructure protection and cybercrime cooperation mechanisms, as well as the establishment of policies, institutions, and resources for participation in regional and international policy debates.
4. **The EU's implementation is most robust where legislative frameworks reflect political commitments through defined duties and compliance expectations, designated authorities, audit or monitoring functions, and built-in enforcement mechanisms.** In the EU's case, this becomes particularly evident for the norms covering areas such as critical infrastructure protection, data protection, cybercrime cooperation, vulnerability management, and supply chain security.
5. **The EU framework has translated positive commitments into regional practice more readily than prohibitive norms.** Given that EU Member States retain primary competence over national security matters, the EU's role in implementing UN cyber norms framed as prohibitions is expectedly limited. EU-level implementation efforts are strongest where the EU can embed behavioral expectations in existing resilience, preparedness, and capacity building frameworks.
6. **Critical infrastructure protection is one of the areas where EU measures aligning with the behavioral expectations reflected in the UN cyber norms are strongest.** Many EU initiatives in this field also closely intersect with related normative objectives, including supply chain security and vulnerability management.
7. **The EU's implementation remains largely implicit and there is a resulting disconnect between European cyber policy efforts and their link to the UN framework**. As

Chapters 4 and 5 show, many EU-level measures substantively align with the UN cyber norms, yet EU institutions and agencies rarely explicitly articulate EU legislation, policies, institutional activities, partnerships, and capacity building initiatives as contributions to the UN framework for responsible state behavior in cyberspace.

Taken together, these takeaways provide a nuanced answer to the question of whether international cyber norms generate a "UN Effect" in the EU context, demonstrating how such an effect may (or may not) manifest itself within the Union's legislative, political, and institutional practices. On the one hand, the implicit nature of the EU's implementation suggests a limited effect, as many measures are not adopted explicitly because of the UN norms but instead reflect broader internal policy priorities and institutional objectives. On the other hand, this may precisely reflect a deeper form of norm diffusion in which most of the behavioral expectations encapsulated in the norms have already become so deeply embedded in governance structures and practices that their normative influence operates at a tacit level.

Implications

Looking beyond the EU's internal dynamics, the EU case also needs to be situated within broader international efforts to operationalize cyber norms. Its implementation experience has not developed in a vacuum, but forms part of a wider set of regional and international efforts to translate agreed behavioral expectations into practice. Comparing these efforts shows that while the EU likely has one of the most mature norms implementation frameworks, many of the same building blocks – including, for example, cybersecurity coordination structures and agencies, strategic cybersecurity frameworks, the establishment of national and EU CSIRTs, and regulatory frameworks addressing critical infrastructure protection and cybercrime cooperation – also feature in other implementation-focused initiatives, including the ASEAN norms implementation checklist, the 2021 OEWG guidance, the OEWG II Chair's voluntary implementation checklist proposal, and relevant UNIDIR research.

This points to growing cross-regional convergence around the practical foundations needed to operationalize the framework. Even though the EU is in many ways unique in its approach to the implementation of the UN cyber norms given its governance and institutional structure that are difficult to replicate elsewhere, its experience can thus also offer insights for other regions and states interested in strengthening implementation:

- **Implementation extends beyond formal declarations, national implementation plans, or projects explicitly labelled as "norms" initiatives.** The EU case illustrates that a narrow understanding of implementation risks overlooking where much of the practical operationalization of the framework already takes place. In a similar vein, many capacity building and reform initiatives in areas such as cybercrime, incident response, certification, data protection, and critical infrastructure protection contribute not only to national policy goals but also to fulfilling agreed international behavioral expectations, even when they are not framed in these terms.

- **Implementation is most effective when anchored in institutions with concrete mandates.** Given that norms are not self-executing, institutional structures and partnerships help embed international behavioral expectations in administrative routines rather than leaving implementation dependent on potentially episodic diplomatic attention. Implementation can therefore benefit from mapping norms not only against laws and policies, but also against institutional responsibilities, identifying which bodies operate in the relevant area, which authorities review compliance, who coordinates assistance, who engages non-governmental actors such as industry, and who feeds implementation lessons back into regional and international discussions.
- **Implementation is not a linear but a dynamic, iterative process.** The EU's experience highlights the importance of built-in revision pathways, including review clauses, periodic reporting, post-incident lessons-learned mechanisms, impact assessments, and institutionalized exchanges between policy, technical, and diplomatic communities. Mechanisms like these can help keep implementation adaptive in response to evolving risks, technologies, and institutional capacities. In turn, domestic and regional practice also helps clarify, refine, and sometimes reshape the meaning of norms. It also demonstrates that there is no single way of operationalizing norms and that states can employ those mechanisms that are best suited to their domestic and/or regional context.
- **Implementation of positive and prohibitive commitments can proceed at different paces.** The EU's case suggests that states and regional bodies may find it easier to make progress on norms that can be embedded in resilience and preparedness frameworks than on norms of a more politically restrictive nature. This sequencing matters particularly for regional implementation strategies because it highlights where early momentum can most likely be leveraged.
- **Critical infrastructure protection constitutes a particularly feasible and politically actionable starting point for broader norm operationalization**. Often, implementation can advance more quickly when tied to concrete public-interest functions such as ensuring the continuity of essential services, strengthening the resilience of financial and energy systems, protecting health services, and maintaining the stability of digital infrastructure.
- **Regional implementation involves balancing common objectives and domestic execution.** Many EU-level legislative and policy instruments often leave precise implementation modalities such as institutional placement, sequencing, budgetary arrangements, and procedural details to Member States, resulting in substantial variation across 27 national systems. This indicates that convergence on regional implementation priorities does not necessarily require identical institutional designs, while at the same time underscoring the importance of having mechanisms in place to compare progress across institutional contexts.

Recommendations for the EU

The findings and reflections outlined in Chapters 6 and 7 have several strategic implications for the EU's future external engagement. In particular, they inform five recommendations for how the EU can follow through on the ambition it expressed at the Global Mechanism's organizational session – namely to "put our words into action on the ground" and make "actionable and tangible progress on the implementation of the UN framework for responsible state behaviour in cyberspace" – into concrete action.[185]

Strengthening internal socialization of the UN framework

Even though implementation is a simultaneous foreign and domestic policy exercise, EU and national actors still discuss UN cyber norms primarily through diplomatic institutions. Given that implementation often depends on actors beyond those circles, closer interaction among different EU stakeholders and communities is essential. Increasing awareness of the UN cyber norms can thus not only improve coherence between EU cyber diplomacy and internal cybersecurity governance but also foster closer interaction among the EU's cyber policy communities. This would also advance the objective set out in the EU's 2020 Cybersecurity Strategy, which called for internal market, law enforcement, diplomatic, and defense communities to work more closely together.[186] This paper has identified concrete links between existing EU instruments and international commitments and highlighted the stakes that different EU-level actors hold in the implementation of cyber norms. Together, these can serve as practical entry points for such internal socialization.

Tracking implementation internally

As a whole-of-government endeavor involving multiple stakeholders, effective operationalization also requires mechanisms to monitor and trace progress across diverse institutional settings without reducing assessment to a binary checklist. A comprehensive account of EU-level implementation, including the role of its capacity building initiatives, can help clarify how responsibilities are distributed, where remaining gaps lie, and how the EU, Member States, and partners can collectively strengthen responsible behavior in cyberspace. Importantly, norms should not only be mapped against laws and policies but also against institutional responsibilities. Building on Recommendation 8.1 above, this approach can help ensure that institutions across different branches of government are aware of their roles and interests in implementation and can coordinate the measures undertaken to that end.

For example, the EU could organize an annual internal "UN norms in EU practice" briefing for relevant agencies and Commission directorates, using one norm, such as the one on critical infrastructure protection, to illustrate how different EU instruments and institutions contribute to its implementation. The Horizontal Working Party on Cyber Issues (HWPCI) and relevant agency boards could carry out similar exercises.

185 Representative of the European Union (2026): Organizational Session, Global Mechanism on ICTs in the Context of International Security, 1st meeting.
186 European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2020): The EU's Cybersecurity Strategy for the Digital Decade.

Learning from other discussions, doing so systematically at the EU level could also generate important dynamics within the Union. In the debate on the applicability of international law in cyberspace, Member States first developed national positions and only later converged on a common EU position. In the case of norms, a comprehensive EU-level account of implementation could work the other way around, stimulating further national mapping exercises and encouraging broader Member State engagement in implementation discussions.

Moving from implicit implementation to explicit external narratives

Demonstrating how existing international commitments are already being operationalized not only has internal benefits. For the EU, making its implementation pathways more explicit is particularly important given that its starting point for norms implementation is different from that of many other countries. Although the situation varies among the UN Member States, all have endorsed the norms and increased their engagement in shaping how the norms are understood and implemented. Communicating how the EU's own regulatory and governance models contribute to these efforts – with the EU's July contribution on norms implementation representing an important first step – can therefore provide a practical reference point, strengthen the EU's role as a partner for dialogue, capacity building, and the exchange of lessons learned, and increase international awareness of the EU's cybersecurity policy ecosystem. This is particularly important at a time when some states continue to question the adequacy of existing norms and international law in cyberspace, for which explicit implementation narratives can provide a concrete counterpoint.

Embedding norms implementation in cyber capacity building

While EU Member States have already underlined the need to better connect the Union's cyber capacity building strategy with the UN norms framework,[187] the examples provided in Chapter 5 indicate that concrete programs only partially reflect the implementation of the framework in their design and delivery. Implementation mapping exercises like this paper offer an evidence base for making that connection more explicit in practice. They can help identify which capacities – for example, incident response, cybercrime investigation, critical infrastructure resilience or participation in international

187 European Union (2022): Council conclusions on the development of the European Union's cyber posture, 9364/22.

processes – are most critical for implementing specific norms and where the EU's external action already addresses these areas. For decision-makers, this should not necessarily mean adopting a top-down approach of translating norms into capabilities. A more effective approach would recognize how fundamental capabilities addressed through capacity building activities, based on the needs of partner countries, can, as a side effect, enable states to implement the substance of UN norms from the bottom up. This means there is no need to reinvent the wheel. Rather, already small but meaningful adjustments in the framing and political embedding of capacity building activities can strengthen the norms implementation lens and help avoid treating norm implementation and cyber capacity building as separate agendas when, in practice, they are deeply intertwined.

Leveraging the UN Global Mechanism and cross-regional platforms as implementation hubs

The launch of the UN Global Mechanism offers several concrete entry points to advance these recommendations. At the UN level, the EU could, for example:

- build on its July contribution by developing and publishing implementation-oriented working papers or mapping notes that show how particular norms (or clusters of norms) are implemented through specific instruments;
- organize side events focused on the implementation of specific norms, such as those on critical infrastructure protection (norms f–h), supply chain security, or assistance;
- facilitate technical briefings by operational actors – such as ENISA, the CSIRTs Network, or relevant regulators – in Mechanism working groups to illustrate how commitments are translated into procedures and institutional practice at the EU level; and
- feed insights from its own experience into any renewed work on a UN voluntary implementation checklist.

In parallel, the EU should deepen cross-regional engagement with norms implementation initiatives developed by other regional organizations, particularly ASEAN and the African Union. This would help identify overlaps, exchange experiences, and develop follow-up cooperation. Joint implementation-focused working papers, informal dialogues, or side events could address specific norms, common implementation challenges, and emerging good practices. The norms relating to critical infrastructure protection provide the most feasible and politically actionable starting point for broader cross-regional norm operationalization and mobilization.

Annex

Annex I: Checklist of possible norms implementation activities

Norm	Possible Norms Implementation Activities
Norm A: Interstate cooperation on security	• Integrating international cooperation as a core pillar of cybersecurity strategies and other strategic or policy documents • Committing to and promoting the Framework for Responsible State Behavior in cyberspace • Establishing a national/regional framework for coordinated response to large-scale cyber incidents and crises • Developing a national or regional procedure for diplomatic responses to malicious cyber activities • Developing a national/regional posture in cyber defense • Articulating a national/regional position on the applicability of international law in the cyber context • Engaging in bilateral, regional, and multilateral cooperation at technical, operational, and diplomatic levels
Norm B: Considering all relevant information in case of ICT incidents	• Designating national CSIRTs, inter alia, responsible for detecting and responding to ICT incidents • Establishing regional technical and operational information-sharing mechanisms, including between national CSIRTs • Introducing incident reporting obligations • Developing capabilities for coordinated regional and intraregional detection and situational awareness of ICT incidents • Articulating a national/regional approach to attribution, including the possible pursuit of joint regional attribution • Seeking the peaceful settlement of disputes arising from ICT incidents • Adopting guidance on the classification of ICT incidents
Norm C: Preventing misuse of ICTs	• Designating national CSIRTs inter alia, responsible for detecting and responding to ICT incidents • Establishing regional information-sharing mechanisms, including between national CSIRTs • Developing capabilities for coordinated regional and intraregional detection and situational awareness of ICT incidents • Criminalizing wrongful acts involving the misuse of ICTs • Adopting standards and procedures concerning the export of cyber-surveillance tools • Articulating a national/regional understanding of the applicability of the principle of due diligence in the cyber context

Norm D: Cooperation to stop crime and terrorism	• Developing a national/regional framework for the criminalization of wrongful acts involving the misuse of ICTs • Developing a national/regional framework to prevent the use of ICTs for terrorist purposes • Establishing national/regional law enforcement institutions and coordination structures to cooperate to stop cybercrime • Adopting rules to facilitate practical cooperation between judicial and law enforcement authorities • Participating in and promoting international instruments to fight criminal and terrorist use of ICTs
Norm E: Respecting human rights and privacy	• Adopting policies and establishing institutions that promote and protect human rights and fundamental freedoms online and offline • Enacting data protection legislation ensuring respect for the right to privacy in the digital age • Adopting legislation governing the use of personal data for law enforcement purposes • Establishing standards and procedures to ensure compliance with human rights obligations when cyber-surveillance items are exported • Articulating a regional position on the applicability of international human rights law in the cyber context
Norm F: Not damaging critical infrastructure	• Putting in place rules and processes for designating critical infrastructure sectors • Articulating a national/regional understanding on the applicability of international law in the cyber context • Developing a national/regional position and doctrine on cyber defense • Establishing a cyber command and regional platforms for cooperation and information exchange between cyber commands and military CSIRTs
Norm G: Protecting critical infrastructure	• Designating critical infrastructure sectors and put in place procedures for identifying critical infrastructure entities • Establishing a regulatory framework for the protection of critical infrastructure • Introducing voluntary, coordinated preparedness testing for highly critical entities • Establishing regional platforms for cooperation and information exchange in the area of critical infrastructure protection • Adopting and testing critical infrastructure-specific crisis and incident management frameworks • Maintaining and supporting the integrity and availability of critical Internet infrastructure
Norm H: Responding to requests for assistance	• Establishing a process for mutual operational assistance, including mutual legal assistance • Introducing a mechanism to cover costs related to the deployment of expert teams in the context of assistance operations • Developing a framework enabling the involvement of the private sector in supporting responses to assistance requests • Establishing a framework for coordinated response to large-scale cyber incidents and crises • Conducting regular cyber exercises to strengthen mutual assistance capabilities

Norm I: Ensuring supply chain security	• Introducing a legal framework requiring specific entities to implement supply chain risk management measures • Creating a cybersecurity certification framework for ICT products • Adopting cybersecurity requirements for products with digital elements through a product safety regulatory framework • Expanding product liability frameworks to ICT products • Integrating supply-chain security provisions within cybersecurity strategies • Conducting and coordinating security risk assessments for critical ICT supply chains • Introducing measures to mitigate cybersecurity risks associated with 5G networks • Articulating an understanding of key ICT supply chain concepts, risk scenarios, and mitigation recommendations • Issuing advisories, guidance, and reports on supply chain security
Norm J: Reporting ICT vulnerabilities	• Integrating vulnerability disclosure provisions within cybersecurity strategies • Designating CSIRTs as coordinated vulnerability disclosure (CVD) coordinators • Establishing regional information-sharing mechanisms and collaboration among CVD coordinators • Introducing a legal framework requiring specific entities to implement vulnerability disclosure and handling measures • Establishing a legal framework addressing vulnerability handling and reporting requirements for products with digital elements • Developing and supporting vulnerability management initiatives • Issuing advisories, guidance, and reports on vulnerability disclosure policies and vulnerability mitigation
Norm K: Not harming emergency response teams	• Establishing a legal framework defining the roles and responsibilities of CSIRTs • Facilitating cooperation among CSIRTs and participation in CSIRT networks • Publishing and maintaining a list of declared national CSIRTs at a regional/international level

Annex II: Overview of EU norms implementation activities

Norm	Examples of EU Norms Implementation Activities	EU Implementation Mechanisms (Non-Exhaustive)	
Norm A: Interstate cooperation on security	Integration of international cooperation as a core pillar of regional cybersecurity strategies, other strategic or policy documents and	Policies	• EU Cybersecurity Strategy • EU Cyber Posture • EU International Digital Strategy

	commitment to and promotion of the Framework for Responsible State Behavior in cyberspace	Institutions and Partnerships	• European External Action Service (EEAS) • European Union Agency for Cybersecurity (ENISA)
	Establishment of a regional framework for coordinated response to large-scale cyber incidents and crises	Legislation	• NIS2 Directive (Directive 2022/2555)
		Policies	• Cyber Blueprint
		Institutions and Partnerships	• EU-CyCLONE
	Development of a regional procedure for diplomatic responses to malicious cyber activities	Policies	• Cyber Diplomacy Toolbox
		Institutions and Partnerships	• EEAS
	Development of a regional posture in cyber defense	Policies	• Military Vision and Strategy on Cyberspace as a Domain of Operations • EU Policy on Cyber Defence • EU Cyber Census
		Institutions and Partnerships	• European Defence Agency (EDA) • Military Computer Emergency Response Team Operational Network (MICNET)
	Articulation of a regional position on the applicability of international law in the cyber context	Policies	• Declaration on a Common Understanding of International Law in Cyberspace
	Involvement in bilateral, regional, and multilateral cooperation at technical, operational, and diplomatic levels.	Policies	• EU Action Plan on Cybersecurity and Artificial Intelligence
		Institutions and Partnerships	• EEAS • ENISA • Cyber dialogues with international partners • Digital Partnerships and Digital Dialogues • EU-LAC Digital Alliance • EU-Western Balkans Regulatory Dialogue • Security and defence partnerships • Organization for Security and Co-operation in Europe

			(OSCE) • NATO • G7 Cybersecurity Working Group • ASEAN Regional Forum
Norm B: Considering all relevant information in case of ICT incidents	Designation of national CSIRTs, inter alia, responsible for detecting and responding to ICT incidents	Legislation	• NIS2 Directive (Directive 2022/2555)
	Establishment of regional information-sharing mechanisms, including between national CSIRTs	Legislation	• NIS2 Directive (Directive 2022/2555) • Cybersecurity Act (Regulation 2019/881)
		Policies	• EU Cyber Posture
		Institutions and Partnerships	• ENISA • CSIRTs Network • EU-CyCLONe • CERT-EU • EEAS with EU INTCEN and Hybrid Fusion Cell
	Enactment of incident reporting obligations	Legislation	• NIS2 Directive (Directive 2022/2555) • Critical Entities Resilience Directive (Directive 2022/2557) • Digital Operational Resilience Act (Regulation 2022/2554) • Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (Delegated Regulation 2024/1366) • Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (Regulation 2023/2841)
		Institutions and Partnerships	• ENISA • NIS Cooperation Group • CSIRTs Network
	Development of capabilities for coordinated regional and intraregional detection and common situational awareness of ICT incidents	Legislation	• Cyber Solidarity Act (Regulation 2025/38)
		Institutions	• Cybersecurity Alert System

		and Partnerships	
	Articulation of a regional approach to attribution, including the possible pursuit of joint regional attribution	Policies	• Cyber Diplomacy Toolbox
		Institutions and Partnerships	• EEAS • Council of EU with HWPCI, PSC, RELEX • Court of Justice of the EU
	Recognition of the need to seek the peaceful settlement of disputes arising from ICT incidents	Policies	• Declaration on a Common Understanding of International Law in Cyberspace
		Institutions and Partnerships	• EEAS
	Adoption of guidance on the classification of ICT incidents	Policies	• Cybersecurity Incident Taxonomy
		Institutions and Partnerships	• NIS Cooperation Group
Norm C: Preventing misuse of ICTs	Designation of national CSIRTs, inter alia, responsible for detecting and responding to ICT incidents	Legislation	• NIS2 Directive (Directive 2022/2555)
	Establishment of regional information-sharing mechanisms, including between national CSIRTs	Legislation	• NIS2 Directive (Directive 2022/2555) • Cybersecurity Act (Regulation 2019/881)
		Policies	• EU Cyber Posture
		Institutions and Partnerships	• ENISA • CSIRTs Network • EU-CyCLONe • CERT-EU • EEAS with EU INTCEN and Hybrid Fusion Cell
	Development of capabilities for coordinated regional and intraregional detection and common situational awareness of ICT incidents	Legislation	• Cyber Solidarity Act (Regulation 2025/38)
		Institutions and Partnerships	• Cybersecurity Alert System
	Criminalization of wrongful acts involving the misuse of ICTs	Legislation	• Directive on attacks against information systems (Directive 2013/40)

			• Directive on combating fraud and counterfeiting of non-cash means of payment (Directive 2019/713) • Directive on combating the sexual exploitation of children online and child pornography (Directive 2011/93)
	Adoption of standards and procedures concerning the export of cyber-surveillance tools	Legislation	• Regulation setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (Regulation 2021/821)
	Articulation of a regional understanding of the applicability of the principle of due diligence in the cyber context	Policies	• Declaration on a Common Understanding of International Law in Cyberspace
		Institutions and Partnerships	• EEAS
Norm D: Cooperation to stop crime and terrorism	Development of a regional framework for the criminalization of wrongful acts involving the misuse of ICTs	Legislation	• Directive on attacks against information systems (Directive 2013/40) • Directive on combating fraud and counterfeiting of non-cash means of payment (Directive 2019/713) • Directive on combating the sexual exploitation of children online and child pornography (Directive 2011/93)
	Development of a regional framework to prevent the use of ICTs for terrorist purposes	Legislation	• Regulation on addressing the dissemination of terrorist content online (Regulation 2021/784)
	Establishment of regional law enforcement actors and coordination structures to cooperate to stop cybercrime	Institutions and Partnerships	• Europol's European Cybercrime Centre (EC3) • Joint Cybercrime Action Taskforce (J-CAT) • European Union Agency for Criminal Justice Cooperation (Eurojust) • European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom,

			Security and Justice (eu-LISA) • European Union Cybercrime Task Force (EUCTF) • European Multidisciplinary Platform Against Criminal Threats (EMPACT)
	Adoption of intraregional rules to facilitate practical cooperation between judicial and law enforcement authorities	Legislation	• Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (Regulation 2023/1543) • Regulation establishing a collaboration platform to support the functioning of joint investigation teams (Regulation 2023/969) • Regulation on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system, Regulation 2022/850)
	Participation in and promotion of international instruments to fight criminal and terrorist use of ICTs	Legislation	• Council of Europe Convention on Cybercrime (Budapest Convention) • UN Convention against Cybercrime
		Institutions and Partnerships	• International Counter Ransomware Initiative • Christchurch Call
Norm E: Respecting human rights and privacy	Commitment to the promotion and protection of human rights and fundamental freedoms online and offline	Legislation	• EU Charter of Fundamental Rights
		Policies	• EU Cybersecurity Strategy • Action Plan on Human Rights and Democracy for years 2020-2027 • Human Rights Guidelines on Freedom of Expression Online and Offline • European Declaration on Digital Rights and Principles

		Institutions and Partnerships	• Court of Justice of the European Union • European Court of Human Rights
	Enactment of data protection legislation ensuring respect for the right to privacy in the digital age	Legislation	• General Data Protection Regulation (Regulation 2016/679)
		Institutions and Partnerships	• European Data Protection Supervisor (EDPS) • European Data Protection Board (EDPB)
	Adoption of legislation governing the use of personal data for law enforcement purposes	Legislation	• Data Protection Law Enforcement Directive (Directive 2016/680)
	Establishment of standards and procedures to ensure compliance with human rights obligations for the export of cyber-surveillance items	Legislation	• Regulation setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (Regulation 2021/821)
		Policies	• Commission Recommendation on guidelines on the export of cyber-surveillance items under Article 5 of Regulation 2021/821
	Articulation of a regional position on the applicability of international human rights law in the cyber context	Policies	• Declaration on a Common Understanding of International Law in Cyberspace
		Institutions and Partnerships	• EEAS
Norm F: Not damaging critical infrastructure	Regional designation of critical infrastructure sectors	Legislation	• NIS2 Directive (Directive 2022/2555) • Critical Entities Resilience Directive (Directive 2022/2557)
	Articulation of a regional understanding on the applicability of international law in the cyber context	Policies	• Declaration on a Common Understanding of International Law in Cyberspace
		Institutions and Partnerships	• EEAS

	Development of a regional posture on cyber defense	Policies	• Military Vision and Strategy on Cyberspace as a Domain of Operations • EU Policy on Cyber Defence • EU Cyber Census
		Institutions and Partnerships	• EDA • MICNET
	Establishment of regional platforms for cooperation and information exchange between cyber commands and military CSIRTs	Policies	• EU Policy on Cyber Defence
		Institutions and Partnerships	• Conference of European Cyber Commanders (CYBERCO) • EU Cyber Defence Coordination Centre (EUCDCC) • MICNET • CSIRTs Network
Norm G: Protecting critical infrastructure	Designation of critical infrastructure sectors and national identification of critical infrastructure entities	Legislation	• NIS2 Directive (Directive 2022/2555) • Critical Entities Resilience Directive (Directive 2022/2557)
	Establishment of a regional regulatory framework for the protection of critical infrastructure	Legislation	• NIS2 Directive (Directive 2022/2555) • Critical Entities Resilience Directive (Directive 2022/2557) • Digital Operational Resilience Act • Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows ((Delegated Regulation 2024/1366) • Commission Implementing Regulation amending Implementing Regulation 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures (Implementing Regulation 2019/1583)
		Policies	• Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors

			• NIS Investments Reports
		Institutions and Partnerships	• ENISA
	Introduction of voluntary, coordinated preparedness testing for highly critical entities	Legislation	• Cyber Solidarity Act (Regulation 2025/38)
	Establishment of regional platforms for cooperation and information exchange in critical infrastructure protection	Legislation	• NIS2 Directive (Directive 2022/2555) • Critical Entities Resilience Directive (Directive 2022/2557)
		Institutions and Partnerships	• NIS Cooperation Group • CSIRTs Network • EU-CyCLONe • Critical Entities Resilience Group (CERG)
	Adoption and testing of critical infrastructure-specific crisis and incident management frameworks	Legislation	• NIS2 Directive (Directive 2022/2555)
		Policies	• Cyber Blueprint • Critical Infrastructure Blueprint
		Institutions and Partnerships	• ENISA
	Support for the integrity and availability of critical Internet infrastructure	Policies	• EU Cybersecurity Strategy
		Institutions and Partnerships	• ENISA
Norm H: Responding to requests for assistance	Establishment of a regional framework for mutual operational assistance between EU Member States, including mutual legal assistance	Legislation	• NIS2 Directive (Directive 2022/2555)
		Policies	• EU Policy on Cyber Defence
		Institutions and Partnerships	• Permanent Structured Cooperation in Security and Defence Policy (PESCO) • Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) • J-CAT
	Introduction of a regional	Legislation	• Cyber Solidarity Act

	mechanism to cover costs related to the deployment of expert teams in the context of Member State-to-Member State mutual assistance operations		(Regulation 2025/38)
	Development of a framework enabling the involvement of the private sector in supporting responses to assistance requests	Legislation	• Cyber Solidarity Act (Regulation 2025/38)
		Institutions and Partnerships	• ENISA
	Establishment of a regional framework for coordinated response to large-scale cyber incidents and crises	Policies	• Cyber Blueprint
	Conduct of regular cyber exercises to strengthen mutual assistance capabilities	Policies	• Strategic Compass for Security and Defence
Norm I: Ensuring supply chain security	Introduction of a legal framework requiring specific entities to implement supply chain risk management measures	Legislation	• NIS2 Directive (Directive 2022/2555)
		Policies	• Technical Implementation Guidance on Commission Implementing Regulation 2024/2690 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures
		Institutions and Partnerships	• ENISA
	Creation of a cybersecurity certification framework for ICT products	Legislation	• Cybersecurity Act (Regulation 2019/881) • Implementing Regulation on the adoption of a European Common Criteria-based cybersecurity certification scheme (Implementing Regulation 2024/482)
		Institutions and Partnerships	• European Cybersecurity Certification Group (ECCG) • Stakeholder Cybersecurity Certification Group (SCCG)

	Adoption of cybersecurity requirements for products with digital elements through a product safety regulatory framework	Legislation	• Cyber Resilience Act (Regulation 2024/2847)
	Expansion of product liability frameworks to ICT products	Legislation	• Product Liability Directive (Directive 2024/2853)
	Integration of supply-chain security provisions within EU Member States' cybersecurity strategies	Legislation	• NIS2 Directive (Directive 2022/2555)
	Coordination of security risk assessments for critical ICT supply chains	Legislation	• NIS2 Directive (Directive 2022/2555)
		Institutions and Partnerships	• NIS Cooperation Group • European Commission • ENISA
	Introduction of regional measures to mitigate cybersecurity risks associated with 5G networks	Policies	• 5G Cybersecurity Toolbox • Coordinated risk assessment of the cybersecurity of 5G networks • Council conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G
		Institutions and Partnerships	• NIS Cooperation Group
	Articulation of a regional understanding of key ICT supply chain concepts, risk scenarios, and mitigation recommendations	Policies	• ICT Supply Chain Security Toolbox • Council conclusions on ICT supply chain security
		Institutions and Partnerships	• NIS Cooperation Group
	Issuance of advisories, guidance, and reports on supply chain security	Institutions and Partnerships	• ENISA
Norm J: Reporting ICT vulnerabilities	Integration of vulnerability disclosure provisions within EU Member States' cybersecurity strategies	Legislation	• NIS2 Directive (Directive 2022/2555)
		Institutions and Partnerships	• ENISA
	Designation of national and EU CSIRTs as coordinated vulnerability disclosure	Legislation	• NIS2 Directive (Directive 2022/2555)

	coordinators		• Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (Regulation 2023/2841)
		Institutions and Partnerships	• ENISA
	Establishment of regional information-sharing mechanisms and collaboration among national coordinated vulnerability disclosure coordinators	Legislation	• NIS2 Directive (Directive 2022/2555)
		Institutions and Partnerships	• CSIRTs Network • NIS Cooperation Group
	Introduction of a legal framework requiring specific entities to implement vulnerability disclosure and handling measures	Legislation	• NIS2 Directive (Directive 2022/2555)
		Policies	• Technical Implementation Guidance on Commission Implementing Regulation 2024/2690 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures
		Institutions and Partnerships	• ENISA
	Establishment of a legal framework addressing vulnerability handling and reporting requirements for products with digital elements	Legislation	• Cyber Resilience Act (Regulation 2024/2847)
		Institutions and Partnerships	• ENISA
	Development and support for vulnerability management initiatives	Legislation	• NIS2 Directive (Directive 2022/2555)
		Institutions and Partnerships	• ENISA • Common Vulnerabilities and Exposures (CVE) program
	Issuance of advisories, guidance, and reports on vulnerability disclosure policies and vulnerability mitigation	Institutions and Partnerships	• ENISA CERT-EU

Norm K: Not harming emergency response teams	Establishment of a legal framework defining the roles and responsibilities of national CSIRTs and CERT-EU	Legislation	• NIS2 Directive (Directive 2022/2555) • Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (Regulation 2023/2841)
	Facilitation of cooperation among CSIRTs and participation in CSIRT networks	Legislation	• NIS2 Directive (Directive 2022/2555)
		Institutions and Partnerships	• Forum for Incident Response and Security Teams (FIRST)
	Publication and maintenance of a list of declared national CSIRTs in the EU	Institutions and Partnerships	• CSIRTs Network

Acknowledgements

The authors would like to thank Cristian Michael Tracci, Eugene Tan, Helene Pleil, Sven Herpig for the time they devoted to providing thorough feedback on earlier drafts of this paper. Any omissions and mistakes are the sole responsibility of the authors. The authors also extend their gratitude to Alina Siebert and Luisa Seeling for their assistance with the editing and layout of this publication.

Research and analysis have not been commissioned by any entity.

Authors

Patryk Pawlak
Part-time Professor, European University Institute & Visiting Scholar, Carnegie Europe
patryk.pawlak@eui.eu

Christina Rupp
Lead International Cybersecurity Policy
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.
c/o Publix
Hermannstraße 90
D-12051 Berlin

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