Policy Paper

Cyber Solidarity in the Making

Is the EU Stepping into NATO's Blind Spot?

| Siim Alatalu |

August 2025

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI · ESTONIA

Title: Cyber Solidarity in the Making: Is the EU Stepping into NATO's Blind Spot?
Authors: Alatalu, Siim
Publication date: August 2025
Category: Policy paper

Cover page photo: An IT specialist looks at a morphological analysis of a software containing a malware at the Lorraine Laboratory for Research in Computer Science and Applications headquarters in Villers-les-Nancy, on 25 October 2023. Jean-Christophe Verhaegen / AFP / Scanpix.

Keywords: capacity building, cybersecurity assistance, cyber defence, interoperability, resilience, EU, NATO

ISSN 2228-2068

63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

Contents

List of Abbreviations

Blue OLEx	Blueprint Operational Level Exercise
CCDCOE	Cooperative Cyber Defence Centre of Excellence (NATO)
CDAC	Cyber Defense Assistance Collaborative
CII	Critical Information Infrastructure
CSIRT	Computer Security Incident Response Teams
CSoA	Cyber Solidarity Act
ECCC	Cybersecurity Competence Centre
EEAS	European External Action Service
ENISA	European Union Agency for Cybersecurity
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
DEP	Digital Europe Programme
LAC4	Latin America and Caribbean Cyber Competence Centre
MS	Member States
NCSC	NATO Cyber Security Centre
NICC	NATO Integrated Cyber Defence Centre
NIS	Network and Information Systems
OAS	Organization of American States
PPP	public-private partnership
SOC	Security Operation Centre
TFEU	Treaty on the Functioning of the European Union
VCISC	Virtual Cyber Incident Support Capability

Acknowledgements

The author would like to thank the officials and experts from the ministries and the national cybersecurity agencies, as well as the European Union institutions, who agreed to be interviewed and share their insights and feedback. The author would also like to extend his sincere gratitude to Ms Maria Kruusement for her invaluable contribution as research assistant to this policy paper, as part of her cybersecurity-focused internship at the ICDS in the summer of 2025.

About the Author

Siim Alatalu

Siim Alatalu joined the ICDS in June 2024 as a cybersecurity fellow, focusing on research and helping steer the Tallinn Digital Summit. Before joining the ICDS, he gained extensive cybersecurity experience in both the private sector and national cyber defence. From early 2022, he led Estonia's national cyber range as CEO of Foundation CR14. His international experience includes serving as the founding Director of EU CyberNet from 2019, working to strengthen global cyber capacity. Prior to that, he was Head of International Relations at the NATO Cooperative Cyber Defence Centre of Excellence from 2015. During the Estonian Presidency of the Council of the European Union in 2017, he also co-led the development of the EU's cyber policy and strategy, as Vice Chair of the Council's Horizontal Working Party for Cyber Issues (HWP). Between 2001 and 2014, Mr Alatalu worked in different positions at the Estonian Ministry of Defence, including serving as a diplomat at the Estonian Delegation to NATO in Brussels, Belgium. Siim Alatalu is a graduate of the Maxwell School of Syracuse University, as well as of the Baltic Defence College and the University of Tartu.

Introduction

Alliances, solidarity, and mutual assistance in security and defence are as old as warfare itself. So, when cyberspace emerged as a new battleground in the early 2000s, it came with a classic question: how should Allies respond when one of them is under digital siege?

NATO first recognised cyber threats at the 2002 Prague Summit, but it was the 2007 state-sponsored attacks on Estonia – widely attributed to Russia – that brought cyber defence firmly onto the North Atlantic Council's table. Since then, the Alliance has wrestled with a central dilemma: can a cyberattack trigger Article 5, and if so, what would a collective response in cyberspace look like? The 2014 Wales Summit moved the discussion forward by stressing that "assistance to Allies should be addressed in accordance with the spirit of solidarity" (para. 72).[1] The 2016 Warsaw Summit went further, declaring cyberspace a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea (para. 70).[2] Yet despite these political commitments and the expansion of shared cyber capabilities, including the NATO Integrated Cyber Defence Centre (NICC) and the NATO Cyber Security Centre (NCSC), the Alliance has remained deliberately vague on thresholds and the precise resources and mechanisms for operationalising collective cyber defence.[3]

While NATO hesitated, the EU pursued a regulatory path on its own, building a comprehensive legal and strategic framework for cybersecurity

While NATO hesitated, the EU pursued a regulatory path on its own, building a comprehensive legal and strategic framework for cybersecurity. As a result, the newly adopted EU Cyber Solidarity Act (CSoA) signals what could become a paradigm shift in its cybersecurity posture – from regulatory to operational. By proposing a pan-European cyber defence infrastructure – including a European Cybersecurity Alert System and a network of interconnected Security Operation Centres (SOC) – the Act hints at developing something the continentally-minded European cyberdefenders have long been missing: a coordinated, high-readiness response capacity. Could this be the EU's first real blueprint for collective cyber defence – and a bold step toward filling what may appear to be a gap in NATO's cyber defence?

The Act hints at developing something the continentally-minded European cyberdefenders have long been missing: a coordinated, high-readiness response capacity

1. What is Cybersecurity Assistance?

The EU today is certainly not a novice in cybersecurity – or in assisting others in strengthening it. Cybersecurity assistance in the European context follows two main tracks: internal, involving support and coordination among EU Member States (MS) and European NATO Allies (work on which might often run in parallel in the capitals); and external, involving cooperation with third countries through enlargement, neighbourhood, or development cooperation frameworks. These external partners may be NATO or EU candidates, party to regional

[1] NATO, *Wales Summit Declaration* (NATO, 4 July 2014).

[2] NATO, *Warsaw Summit Communiqué* (NATO, 9 July 2016).

[3] NATO, "Allies agree new NATO Integrated Cyber Defence Centre," 10 July 2024; NATO, "NATO Cyber Security Centre," accessed in July 2025.

political or defence collaboration dialogues, or recipients of development aid.

The definition of "cybersecurity assistance" can vary widely. It may involve operational support during cyber incidents, technical capacity-building, intelligence and threat information sharing, or longer-term collaboration on cyber norms, joint research, and interoperability. Assistance also serves different strategic goals: enhancing resilience, promoting alignment on foreign policy, or ensuring that partners can securely integrate with EU or NATO systems.

Within the EU, one of the most common forms of internal cyber assistance is information sharing, largely coordinated by the European Union Agency for Cybersecurity (ENISA) and involving the MS' national Computer Security Incident Response Teams (CSIRT).[4] During the past decade, several formats have emerged to support Member State cooperation, including the CSIRT Network, the Network and Information Systems (NIS) Cooperation Group, and the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe).[5] Adding to many high-level cybersecurity agreements, they reflect a growing recognition that cybersecurity cannot be managed in isolation but as a collaborative and solidary effort.[6] The 2025 CSoA, therefore, builds on a broad foundation, signalling a shared interest in stronger joint preparedness and operational solidarity among MS.

Unlike the EU, NATO does not build shared capabilities this way. While "cyber defence is part of NATO's core task of deterrence and defence," it acts more like a 'glue' between nationally owned assets and capabilities, while also setting planning targets that the Alliance should collectively meet.[7] In this context, NATO has also taken steps toward collective cyber assistance. At the 2023 Vilnius Summit, Allies agreed to launch a Virtual Cyber Incident Support Capability (VCISC) – a multilateral mechanism designed to assist members under cyberattack. This capability was tested for the first time in an exercise in April 2025, marking a significant operational milestone.

NATO acts like a 'glue' between nationally owned assets and capabilities, while also setting planning targets that the Alliance should collectively meet

Beyond NATO and the EU, other international bodies, too, have been active in the area of enhancing solidarity in cybersecurity affairs. The United Nations has spent more than a decade promoting international norms for responsible state behaviour in cyberspace, concluding with the recent Open-Ended Working Group's Final Report in 2025.[8] The OSCE has developed confidence-building measures to reduce cyber tensions and prevent escalation.[9]

2. Deep Dive: The Cyber Solidarity Act

The EU Cyber Solidarity Act, adopted in 2025, marks a paradigm shift – from enhancing coordination to building operational capabilities. While earlier EU initiatives have emphasised harmonisation of national frameworks and information sharing, the CSoA introduces operational tools intended to enable joint detection, response, and recovery in the face of major cross-border cyber

[4] ENISA, "What is a CSIRT and how can it help me?," 4 May 2020; European Union, "European Union Agency for Cybersecurity (ENISA)," accessed in July 2025.

[5] CSIRTs Network, "CSIRTs Network," accessed in July 2025; European Commission, "NIS Cooperation Group," accessed in July 2025; ENISA, "EU CyCLONe," accessed in July 2025.

[6] Examples of EU cybersecurity strategies that inter alia promote solidarity between MS include the first EU Cybersecurity Strategy (2013) and the proposal for the Network and Information Security (NIS) Directive, which became the first EU-wide cybersecurity law in 2019. The NIS2 Directive (2024) further expanded cybersecurity requirements. Other initiatives include the EU Cyber Diplomacy Toolbox (2017), enabling coordinated responses to major cyber incidents; the EU Cybersecurity Strategy (2020), aiming for a resilient and sovereign digital Europe by 2030; and the Joint Cyber Defence Communication (2022), supporting a coherent EU-level cyber defence policy.

[7] Allied Command Transformation NATO's Strategic Warfare Development Command, "Cyber Defence," accessed in July 2025.

[8] Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025, *Open-ended working group on security of and in the use of information and communications technologies 2021-2025. Draft Final Report* (United Nations General Assembly, 11 July 2025).

[9] OSCE Secretariat, Transnational Threats Department, *10 Years of OSCE Cyber/ICT Security Confidence-Building Measures* (Organization for Security and Co-operation in Europe, 24 October 2023).

threats. Unlike other acts in the cybersecurity domain, the CSoA is not based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), but has a dual legal basis, namely Article 173(3) and Article 322(1)(a) of the TFEU.[10]

The EU Cyber Solidarity Act marks a paradigm shift from enhancing coordination to building operational capabilities

According to interviews conducted for this policy paper, the road to consensus between the MS and the European Commission (EC) was not a short one. Initially lacking an impact assessment, it had been somewhat unclear what concrete problem the EC's new initiative was to solve after it was first published in the EU Policy on Cyber Defence in 2022.[11] In parallel, Russia's military aggression against an EU candidate country, Ukraine, also clearly showed the need for more European solidarity across the board, including in cybersecurity.

The CSoA's objective is to strengthen EU-wide cybersecurity preparedness and solidarity through three main pillars:

- **European Cybersecurity Alert System** – a real-time, EU-level detection and alert mechanism that is based on a network of interconnected SOCs across MS. Supported by AI and advanced analytics, these SOCs aim to improve situational awareness and help coordinate early responses to emerging threats.

- **Cybersecurity Emergency Mechanism** that provides structured assistance to MS under cyberattack in three ways: support preparedness actions, create an EU Cybersecurity Reserve of trusted cybersecurity providers, and ensure mutual assistance as a coordinated recovery action.

- **Cybersecurity Testing and Certification Infrastructure** that supports the EU's efforts to strengthen supply chain security and strategic autonomy, with an emphasis on high-assurance certification schemes for critical products and services.

With some generalisation, the CSoA offers MS support to develop concrete tools for mutual aid, backed by EU funding and managed through pre-established coordination structures. Achieving a functional capability that is ready and available for the EU and MS, however, would take at best a few years and would also require untraditional thinking that, in addition to sovereign MS, the EU could play the role of a driver of operational cybersecurity.

The CSoA offers Member States support to develop concrete tools for mutual aid, backed by EU funding and managed through pre-established coordination structures

According to experts interviewed, the creation of new regional cyberhubs sparked questions about the actual need for additional entities and their possible locations – as well as the concern of added layers of duplication. Yet, in principle, proposals like the cybersecurity reserve and regional cross-border cyberhubs, based on existing CSIRTs that allow groups of countries (at a minimum of 3 MS) to pursue the course together with generous EU funding (up to 75% of costs), could also have a positive impact. MS have to date responded to these with different levels of enthusiasm. On one hand, the Nordic and Baltic countries have already agreed to collaborate by contributing to a regional hub based in Denmark, whereas other countries currently do not have such an intent at all.

While the cyberhubs would share information related to cyber threats and support EU MS in rapid response to those, they are also important beyond the borders of the EU. Namely, they assist third countries that are part of the Digital Europe Programme (DEP), which would have access to the Reserve. These countries include Moldova, which has been part of the DEP since 2024 and has recently signed an amendment that will allow

[10] Susanna Villani, "The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System," *European Journal of Risk Regulation* 16 (2025): 1–13.

[11] European Commission, *Joint Communication To The European Parliament And The Council EU Policy on Cyber Defence* (Brussels, 10 November 2022).

it to access the Reserve.[12] The CSoA also seeks to find ways to include Ukraine, and thus is seen as a contribution to broader security and defence policy in the region.

Compared to previous agreements on cybersecurity collaboration in the EU, the CSoA "adds real-time monitoring and intelligence sharing, something that NIS2 did not mandate."[13] It has also been noted that while NIS2 gave a baseline framework for security risk management, thus focusing on compliance within organisations, the CSoA intends to help tighten the assistance between EU countries in case of a large-scale cyber incident. This is seen to fill the EU-identified gap in "real-time incident response, cross-border solidarity, and coordinated cyber defence."[14]

The CSoA intends to help tighten the assistance between EU countries in case of a large-scale cyber incident

Successful implementation of the CSoA will require significant effort and will to collaborate from both the MS and the cybersecurity industry. Interviewees inter alia highlighted that the complexity of standard EU procedures for calls of interest may be too demanding for the industry and individual enterprises to respond. This is especially pertinent in smaller MS where SME-sized cybersecurity companies may simply lack the required capacity to contribute and deliver the expected service. Interviewees in the different MS capitals acknowledged that they all had a list of the "usual suspects" (i.e., capable cybersecurity companies in their countries) whom they would gladly see as contributors – but who are yet to express any interest.

3. From Paper to Practice

Practice makes perfect, and the CSoA, therefore, raises the question of whether and how its readiness could, in principle, be tested for operationality. Fortunately, over the past decade, MS have already grown used to honing their cyber skills across tactical/technical, operational, and strategic level exercises – under the auspices of, for example, ENISA or the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). To the CSoA, the following exercises would serve as good examples.

- **Blue OLEx & CySOPex: Building a European Cybercrisis Response Culture**. ENISA's annual Blue OLEx and CySOPex exercises test the EU's cyber crisis coordination across technical and strategic decision-making layers. Blueprint Operational Level Exercise (Blue OLEx) series started in 2019 and focus on high-level preparedness, crisis management, and decision-making during simulated cyber crises, involving officials from the CSIRT Network, national cyber-policymakers, and the European Commission via EU-CyCLONe.[15] In 2024, for instance, the Rome-based iteration tested escalation criteria and situational awareness among senior cyber leaders, with technical observers present.[16] Cyber Europe exercise series began in 2012, and is an equivalent effort by ENISA that additionally includes operators from sectors targeted by the exercise scenario (e.g., healthcare in 2022, energy in 2024).

- **NATO VCISC Activation Exercise**. When considering any type of cyber assistance to MS, the NATO VCISC, first tested in April 2025, would also serve as a good example for the EU.[17] Hosted by the Czech Republic, a total of 20 NATO countries participated in a large-scale exercise to test the VCISC. Launched at the 2023 Vilnius Summit, the VCISC links Allies requesting cyber incident support with other NATO states offering resources in areas like malware analysis, digital forensics, and threat intelligence. The

[12] European Commission, "Moldova moves closer to joining the EU Cybersecurity Reserve," 20 May 2025.

[13] EU Cyber Solidarity Act, "Cyber Solidarity Act. Updates, Compliance," accessed in July 2025.

[14] EU Cyber Solidarity Act.

[15] European Commission, *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises* (Official Journal of the European Union, 13 September 2017).

[16] ENISA, "BlueOLEx 2024 exercise: EU-CyCLONe test its cyber crisis response preparedness," 8 November 2024.

[17] NATO, "Allies practise coordination of mutual cyber support through NATO," 14 April 2025.

exercise aimed to ensure rapid, coordinated responses to critical national infrastructure threats. While it demonstrated improved inter-Allied preparedness, participants of the exercise interviewed for this policy paper noted that since this platform works on a senior level, it is essential that decision makers are aware of the VCISC and use it as a whole-of-government tool. The role of NATO HQ and the International Staff (the EC, respectively) was to serve as a clearinghouse – receiving support requests and connecting them with countries that have offered to help – ensuring that Allies know whom to contact when facing a major cyberattack. However, it was also mentioned that nations remained careful from the perspective of allowing other country experts access to national Critical Information Infrastructure (CII), which is often in private ownership.

Another aspect of what makes the VCISC a good example for the EU is that it works on a voluntary basis, like the initiatives proposed by the CSoA, and is reserved for significant incidents – that go beyond casual disruptions and may exceed a nation's own capabilities or involve niche technical requirements. The VCISC works as a virtual mechanism, avoiding the need for physical deployment, diplomatic clearances, or boots on the ground. This allows for faster and more flexible assistance. Support can range from consultations to forensics or malware analysis, but the nature and scope of assistance depend on the requester and the willingness of the supporting ally.

As the CSoA moves on with the implementation of concrete provisions for SOC cooperation, private-sector responders, and incident review protocols, nevertheless, to date, no documented instances of real-world deployment have been confirmed. Exercises and SOC pilots under the Digital Europe Programme are underway, building technical and organisational foundations – but full operational deployment during an actual crisis remains to be demonstrated.[18]

[18] European Commission, "Cybersecurity: EU launches first phase of deployment of the European infrastructure of cross-border security operations centres," 24 November 2022.

4. Don't Send Sympathy – Send Solutions

It has been claimed that the activation of the CSIRT Network and information sharing between the MS' CSIRTs in 2017 possibly saved at least some from major damages from the ongoing WannaCry and NotPetya malware attacks.[19] These episodes revealed that Europe at the time lacked a rapid, unified cybersecurity crisis mechanism. Nevertheless, the need for raising the game and establishing a common reserve and the capacity for a more rapid response to cyberattacks between MS was highlighted even more recently with the SolarWinds attack in 2020, which affected multiple EU-based entities.[20] It has been argued that had the Cyber Solidarity Act already existed back then, it could have served to mitigate the impact on critical infrastructure, whilst ensuring a more coherent approach across MS.[21]

Today, the need for proactive solutions is even more dire due to increased unpredictability. For instance, in early 2025, the United States Secretary of Defence abruptly halted US Cybercommand's ongoing cybersecurity assistance to Ukraine, creating a vacuum in support for a NATO partner country under aggression on both conventional and digital battlegrounds, undermining Ukraine's ability to sustain Russia's attacks – if even not surrendering America's own cyber defences and creating uncertainty about those of NATO.[22]

Recognising this risk, the EU and MS have taken a step forward with the creation of the Tallinn Mechanism – a coordinated platform launched in 2023 to organise and channel cyber assistance to Ukraine. Spearheaded by Estonia and supported by the European External Action Service (EEAS), the Tallinn

[19] CloudFlare, "What was the WannaCry ransomware attack?," accessed in July 2025; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22 August 2018.

[20] Dina A. Temple-Raston, "Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack," *NPR*, 16 April 2021.

[21] Villani, "The Cyber Solidarity Act."

[22] Siim Alatalu, "Is America surrendering its first line of cyber defence?," *ICDS*, 10 March 2025.

Mechanism brings together EU MS, agencies, and key partners to match Ukraine's urgent cybersecurity needs with concrete support. It has already enabled the delivery of advanced cyber threat detection tools, incident response training, and advisory services to Ukrainian institutions.[23]

The Tallinn Mechanism and the CSoA represent a nascent European cyber assistance doctrine that emphasises collective action over bilateral sympathy

What makes the Tallinn Mechanism significant in the context of this policy paper is that it mirrors the logic of the CSoA: rapid response, pooled expertise, and supranational coordination. Together, they represent a nascent European cyber assistance doctrine – one that emphasises collective action over bilateral sympathy.

The CSoA provides the EU with its first mechanism for responding to major cross-border cyber incidents that concurrently includes operational response capability and the required funding to develop it. It allows the EC, following an MS notification, to trigger partial or full-scale responses involving ENISA, the CSIRT Network, and the newly established Cybersecurity Reserve. This reserve, composed of certified private-sector providers, can be deployed for both containment and the initial recovery phase. Crucially, Digital Europe Programme countries outside the EU – like Ukraine – can also benefit from this support.

The Tallinn Mechanism has laid the groundwork, and the Cyber Solidarity Act can scale it to form the backbone of a robust, sovereign, and values-driven European cyber assistance policy

Yet several practical challenges remain. The Act depends on MS' willingness to share sensitive information, which is not always forthcoming. Smaller countries have also voiced concern that the certification process and the overregulation of qualifications for the Reserve may favour large cybersecurity firms from wealthier states, potentially limiting broad participation.

Still, these mechanisms are timely and vital. With the US retreating from its former leadership in cyber capacity building, particularly in Eastern Europe, Europe must now lead where others have stepped back. The Tallinn Mechanism has laid the groundwork, and the Cyber Solidarity Act can scale it. Together, they could form the backbone of a robust, sovereign, and values-driven European cyber assistance policy.

Like in conventional battlegrounds, solidarity in cyberspace must be actionable. As Ukraine's president Volodymyr Zelenskyy famously said on the eve of Russia's full-scale invasion: "I do not need a ride – I need ammo."

5. Cyber Solidarity – Already Actionable?

While the EU's primary focus in cybersecurity remains on internal market regulation – guided by the mutual defence clause (Article 42.7 of the Treaty on European Union) and the solidarity clause (Article 222 of the TFEU) – over time, it has also emerged as the world's largest donor of development cooperation, including in the area of external cybersecurity assistance where the EU and its MS are estimated to have collectively invested approximately €131 million in ongoing cyber capacity building projects.[24]

This assistance primarily takes the form of cyber capacity building, with the EU having launched numerous projects over the years aimed at strengthening the institutional capabilities and skills of national authorities and other cybersecurity stakeholders. Among the most prominent

[23] European Union External Action, "A Year of Cyber Support for Ukraine: The Tallinn Mechanism's Milestone," 19 December 2024.

[24] European Commission, "International development aid," accessed in July 2025; EU CyberNet, "CBB project mapping," accessed in July 2025.

EU-led initiatives today are EU CyberNet and the Latin America and Caribbean Cyber Competence Centre (LAC4).[25]

Unlike, for example, the People's Republic of China, which typically supports third countries through IT infrastructure development, the EU follows a softer, skill-based approach focused on governance, institutional development, and resilience. This strategy also differs from that of other like-minded democracies, such as the United States or the United Kingdom, which deliver cybersecurity capacity-building assistance primarily through technological solutions (e.g., software, toolkits) and training, often via multilateral frameworks such as the Organization of American States (OAS) or the Commonwealth.[26]

The EU follows a softer, skill-based approach focused on governance, institutional development, and resilience

Since the start of Russia's full-scale war against Ukraine in 2022, the EU has mobilised both bilateral and multilateral assistance to support Kyiv's cyber resilience. This cooperation has resulted in the creation of new coordination frameworks, including:

- The Tallinn Mechanism (established in 2023), which brings together 11 countries to coordinate equipment delivery, training, and incident response, with active support from the EU and NATO.[27]
- The IT Coalition for Ukraine, a separate initiative uniting 10 European countries focused on strengthening IT, communication, and cybersecurity capacities.[28]

In addition, the EU has:

- Deployed cyber labs and training centres under the European Peace Facility;[29]
- Provided rapid cyber incident response capabilities;
- Supported Ukraine's legislative alignment with EU cybersecurity frameworks, considering its EU accession goals.[30]

Meanwhile, the United States has played a complementary role, leading its support through the Cyber Defense Assistance Collaborative (CDAC).[31] The CDAC has delivered over $40 million in aid, including 2 600 cyber defence tools and 1 600 training sessions to 24 Ukrainian entities. The initiative fosters public-private cooperation, involving more than 50 organisations, and underscores the importance of collective international action in the cyber domain.

These figures, however, pale in comparison to the resources that the EU has been investing in the Digital Europe Programme (i.e., €8.1 billion within the current Multiannual Financial Framework 2021-27) and cybersecurity therein.[32] Not to mention global cybersecurity spending as such, which is forecasted to increase to nearly €185 billion ($213 billion) in 2025 from €167 billion ($193 billion) in 2024, according to Gartner.[33]

The following graph summarises the context into which the CSoA fits, related to the EU's other cybersecurity initiatives that deal with funding, capacity development, technical standards and certification, and the Union's external relations – in practice, all critical enablers if not pre-requirements for solidarity.

[25] EU CyberNet, "EU CyberNet – the bridge to cybersecurity expertise in the European Union," accessed in July 2025; Latin America and Caribbean Cyber Competence Centre LAC4, "The Bridge to cyber capacity building in the Americas," accessed in July 2025.

[26] Organization of American States, "Cybersecurity Program," accessed in July 2025.

[27] European External Action Service, "A Year of Cyber Support to Ukraine: The Tallinn Mechanism as a Milestone," 19 December 2024.

[28] Dmytro Basmat, "European coalition agrees to aid Ukraine's IT, cybersecurity defense capabilities," *The Kyiv Independent*, 15 February 2024.

[29] EU4Dgital, "European Union strengthens Ukraine's cyber resilience," 24 April 2024.

[30] European Cybersecurity Competence Centre, "Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue," 29 September 2022.

[31] Greg Rattray, Seungmin (Helen) Lee, and Yamen Huq, *Cyber Defense Assistance And Ukraine Lessons And Moving Forward* (Aspen Institute, April 2025).

[32] European Commission, "The Digital Europe Programme," accessed in July 2025.

[33] Gartner, "Gartner Forecasts Worldwide End-User Spending on Information Security to Total $213 Billion in 2025," 29 July 2025.

Instrument/Initiative	Type of Assistance	Beneficiary	Description
Digital Europe Programme (DEP)	Cybercapacity building, financial support	EU Member States and countries associated with DEP	Provides large-scale funding for cybersecurity infrastructure and cross-border cooperation
European Cybersecurity Competence Centre (ECCC) and Network	Funding coordination, research and innovation support	EU MS	Increases Europe's cybersecurity capabilities and competitiveness; manages cybersecurity funding from DEP and Horizon Europe
Cybersecurity Act	Regulatory and institutional support	EU MS	Establishes EU-wide certification schemes and security standards for cybersecurity governance
Cyber Solidarity Act	Cross-border and public-private collaboration to support readiness for emergency response	EU MS and countries associated with DEP	Enables cross-border and public-private collaboration to enhance readiness and capacity for coordinated emergency response to large-scale cyber incidents
Cyber Diplomacy Toolbox	Strategic, political response; Diplomatic tools: preventive, cooperative, stabilising, restrictive (cyber sanctions)	Global, particularly the EU's neighbourhood and strategic partners	Enables coordinated EU diplomatic response to malicious cyber activities and contributes to conflict prevention

Table 1. The CSoA in relation to the EU's cybersecurity initiatives. *Source:* Author.

Conclusion and Recommendations

Solidarity with one's allies is *sine qua non* in cybersecurity ever since large-scale cyberattacks like WannaCry, NotPetya, and SolarWinds revealed the limits of national-only responses. With the Cyber Solidarity Act, the EU has set a clear goal to move from expressions of support to fast, coordinated, and cross-border action. It is in a good position to do so, as over the past decade, the EU has already built active collaboration networks between CSIRTs and conducted countless cybersecurity exercises. The CSoA, in principle, provides a promising framework: centralised activation via the EC, support from ENISA, and a Cybersecurity Reserve of certified private-sector providers from around the MS. Still, the CSoA's eventual success will depend on the Member States' readiness and willingness to contribute – and this should be recognised by European institutions. In August 2025, the Commission mandated ENISA to administer the EU Cybersecurity Reserve with a €36 million budget under the DEP, which is essentially the first real operationalisation of the CSoA.E[34]

The CSoA's eventual success will depend on the Member States' readiness and willingness to contribute

Another reckoning should be that for Europe, cybersecurity solidarity needs to extend beyond the current limits of the EU. First and foremost, NATO's ability to deliver in a cyber-Article-5 situation and the transatlantic link remain another *sine qua non*. NATO's lessons from the VSISC exercise indicate that dire straits in national cybersecurity will not be a military-only situation, and a whole-of-government approach – an EU strength – will be required for mitigating any adverse effects.

From both organisations' perspective, it will remain essential to continue supporting countries that aspire to both EU and NATO membership. The examples of the Tallinn Mechanism and the IT Coalition for Ukraine show how support for like-minded and candidate countries can be scaled up. The CSoA, through

[34] ENISA, "ENISA to operate the EU Cybersecurity Reserve with EUR 36 million," 26 August 2025.

the Digital Europe Programme and its generous funding, could become a platform for the EU's structured external engagements with key partner countries. From the mentioned €36 million, the ENISA-managed Reserve will fund incident response services from trusted providers, deployable in critical sectors like energy and healthcare – and, under specific conditions, even for third countries associated with the DEP.

The CSoA could become a platform for the EU's structured external engagements with key partner countries

Modern cybersecurity is impossible without the private sector. Cybersecurity companies often detect and mitigate threats faster than states. Their infrastructure and intelligence must be integrated into national and EU-level strategies through structured public–private partnerships (PPP). Yet, for the CSoA to succeed, the EU and MS should be aware of the bureaucratic hurdles that might deter some of the capable players from contributing to its initiatives, possibly thereby sabotaging the enthusiasm and the hoped-for solidarity. Therefore, key recommendations for strengthening cyber solidarity in Europe are as follows:

- **Operationalise the Cyber Solidarity Act** by finalising its operational structures and fostering Member States' commitment to ensure rapid, coordinated, and cross-border response capacity.
- **Strengthen EU–NATO coordination** by developing joint protocols and exercises, recognising that cyber crises – particularly those near the threshold of invoking Article 5 – demand integrated military and civilian responses.
- **Extend solidarity beyond EU borders by using** the CSoA and instruments like the Digital Europe Programme to support EU candidates and like-minded countries, building on the success of the Tallinn Mechanism and IT Coalition for Ukraine.
- **Make the CSoA a landmark public–private partnership** by integrating private cybersecurity providers into EU and national practice, recognising their frontline role in detecting and mitigating threats and their contribution to MS' sovereign cyber capacities.
- **Minimise bureaucratic barriers** by streamlining certification and procurement processes under the CSoA to attract capable, innovative private-sector contributors – particularly from smaller MS and their rapidly developing defence industries.
- **Leverage existing networks and exercises** by building on the past decade of CSIRT cooperation and EU-wide cybersecurity exercises to develop mature, interoperable, and tested solidarity mechanisms.

RECENT ICDS PUBLICATIONS

REPORTS

Jermalavičius, Tomas, Henry Rõigas, Oleksandr Sukhodolia, and Dmitri Teperik. ***The Staying Power of Ukrainian Lights. Lessons of Wartime Resilience of the Electricity Sector***. May 2025.

Arjakas, Merili, Kai Kaarelson, Solveig Niitra, Hille Hanso, Ivan U.K. Lyszcz. ***Eesti roll muutuvas rahvusvahelise arengukoostöö arhitektuuris*** [Estonia's Role In the Changing Architecture of International Development Cooperation]. March 2025.

Klyszcz, Ivan U.K., Tony Lawrence, Eric Chan, Jyun-yi Lee. ***Deterrence and Hybrid Warfare: Lessons from Russia's War in Ukraine for Taiwan and the Nordic-Baltic Regio***n. February 2025.

Hosaka, Sanshiro. ***A Mountain to Climb: Russia's Influence in the South Caucasus and EU Policy Options***. January 2025.

Gretskiy, Igor. ***New Russian Immigration to the EU: The Case of the Baltic States, Finland, Germany & Poland***. October 2024.

Atanassova-Cornelis, Elena, Takuya Matsuda, Bart Gaens, and Nele Loorents. ***Japan, NATO, and the Diversification of Security Partnerships***. September 2024.

POLICY PAPERS

Lawrence, Tony, Felix Gasper, and Dick Zandee. "**Defending Europe's Skies: Challenges and Prospects**." May 2025.

Klyszcz, Ivan U.K."**Distance is Not a Shield. Russia's Transnational Repression in Wartime**," May 2025.

Praks, Henrik. "**Russia's Hybrid Attacks in Europe: From Deterrence to Attribution to Response.**" April 2025.

Loorents, Nele, and Jun Nagashima. "**Bridging Two Oceans: The Evolving NATO-Japan Relationship**." July 2024.

ANALYSES

Gasper, Felix, Lukas Mugele. "**Forward Defence in the Cold War.**" August 2025.

Leveque, Arthur, and Justin Leveque. "**Foreign Interference in Distant Territories: French Territories on Azerbaijan's, Russia's, and China's radars**." August 2025.

Larsen, Henrik. "**Toward a Europeanised NATO**." June 2025.

Hanso, Toomas. "**Central Asia's New Railways: Russia's Pain, China's Gain**." March 2025.

Alatalu, Siim. "**The EU's NIS2 Directive A Business Opportunity for the Defence Sector**." March 2025.

Peterson, Annabel. "**The Enemy Within: Russians in Ukrainian Army Ranks and the Fracturing of Post-Soviet Identity**." February 2025.

Idarand, Tõnis. "**For as Long as It Works: Russia's Nuclear Signalling During Its War in Ukraine**." January 2025

BRIEFS

Hosaka, Sanshiro. "**Trump-Brokered Azerbaijan-Armenia Peace Deal: Breakthrough or Another Geopolitical Conundrum?**" August 2025.

Kimoita, Stephen. "**Kenya's Foreign Policy Towards Europe and Estonia**." July 2025.

Huminski, Joshua C., Tony Lawrence, Marianne Paire, Nele Loorents, Katarzyna Zysk, Felix Gasper, ***Hague Summit Series***. June 2025.

Leveque, Arthur, and Justin Leveqye. "***Francophonie: A Subtle Response to Revisionist Powers***." May 2025.

Nazarov, Mykola. "**Returning Ukrainians Home: Mission Possible?**" May 2025.

Maksak, Hennadiy, and Laurynas Jonavičius. ***Russia's War in Ukraine Series***. May 2025.

All ICDS publications are available from https://icds.ee/category/publications/.

ICDS.Tallinn
@ICDS-TALLINN.BSKY.SOCIAL
@ICDS _ Tallinn
ICDS-Tallinn
www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-2068