EU Vision in Cybersecurity: Beyond Rules, Towards Protection

KEY POINTS

1. Common rules do not guarantee uniform implementation. Although the EU has common cybersecurity rules, practice differs significantly between countries. This disconnect weakens the EU's cyber defence shield and leaves the system vulnerable.

2. The shortage of expert personnel and budget is a major problem. Standards keep rising on paper, but many institutions struggle to find competent staff. This lack of resources directly manifests as a security vulnerability.

3. Setting rules is not enough. Stricter controls, technical assistance to institutions and joint cyber exercises between countries are needed so that rules provide real protection.

Summary

This study examines the question: *"Despite common legislation such as the NIS2 Directive, what factors prevent the creation of a homogeneous cybersecurity shield across the EU and create differences in implementation among member states?"*

The main hypothesis is that even with the most perfect cybersecurity law, it will remain only on paper unless there is the technical infrastructure, domestic software and secure servers to implement it. Although the NIS2 Directive aims for a common standard, there is a serious disconnect between legal obligations and practical application. According to the European Commission, as of 7 May 2025, 19 member states had not yet completed the integration of the directive into their domestic law.

The ENISA report of 2025 shows that the problem is not only bureaucratic but also structural: 76% of organisations have difficulty in hiring experts and 71% in retaining them. This confirms that even if common standards are introduced, there is a significant gap in infrastructure, servers and human resources to implement them.

To prevent legal requirements from remaining merely on paper, the EU should tighten its oversight of member states, provide direct financial and technical support to organisations with limited infrastructure and budgets so that they can acquire secure servers using local software, and maximise cyber cooperation through joint exercises and real-time information-sharing networks.

Keywords: Cybersecurity; NIS2 Directive; EU security policy

EU Cybersecurity Framework: Common Rules, Different Practices

Today, everything from hospitals to electricity grids operates through interconnected digital systems. A cyberattack on a network in one country can cross borders and negatively impact neighbouring countries. Cybersecurity therefore cannot be viewed as the responsibility of a single state; it is a common problem affecting Europe as a whole. This is where the NIS2 Directive (Directive (EU) 2022/2555) comes into play. Its main goal is to raise the level of cybersecurity across the EU to a specific and high standard. Compared to previous regulations, it significantly increases the sectors covered and makes the rules much stricter on issues such as risk management by companies, reporting of cyber incidents, and the responsibilities of managers.

However, creating common legislation that looks very good on paper is only the beginning. According to the European Commission's statement of May 2025, 19 member states have not yet integrated this directive into their national law and completed the necessary notifications[1]. This shows that even with common rules, the same quality of implementation cannot be achieved in every country. Cyber threats do not need passports or borders; a security vulnerability in one place can have a chain reaction and affect everyone. The EU's success therefore lies not only in making common decisions, but also in implementing them with the same determination in every member state.

Key Problems: Expertise, Resources and Implementation Gaps

One of the biggest contradictions in the EU's cybersecurity policy is the gap between the rules on paper and the power to implement them in the field. For a state or company to comply with strict rules, good intentions are not enough; it needs a serious team of experts, technical infrastructure and money.

ENISA's *NIS Investments 2025* report points precisely to this problem[3]. According to a large survey of 1,080 experts across Europe, finding and retaining cybersecurity professionals is a real struggle. 76% of participating organisations reported serious difficulties hiring new experts, while 71% reported serious difficulties retaining existing employees.

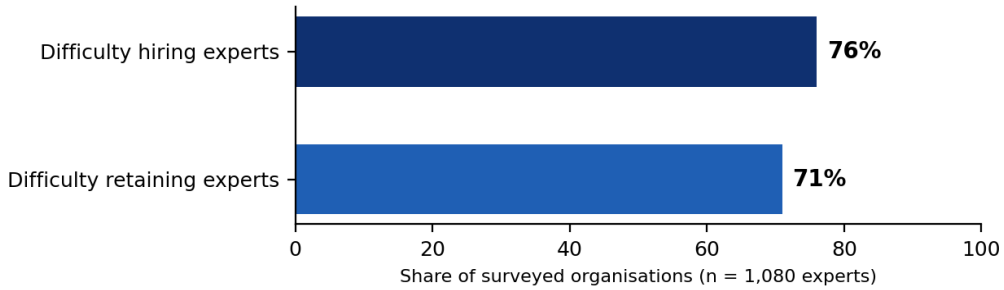

Figure 1: Cybersecurity workforce challenges among surveyed organisations. Source: ENISA, NIS Investments 2025[3].

Small businesses and organisations with limited budgets suffer the most. Lacking funds, they can neither employ qualified personnel, nor update their systems, nor provide proper training for their employees. A company officially signing a document stating "we comply with the law" does not mean that it is truly safe. In my opinion, the real problem is not the lack of a common set of rules in the EU; it is the unfair distribution of capacity to implement these rules among countries and companies. If the EU administration keeps imposing new responsibilities but neglects the human resources and budget aspects, then despite the strictest rules, we will all remain easy targets because of the weak links.

What needs to change

The following recommendations are targeted towards the European Commission, working hand in hand with ENISA and national cybersecurity agencies. To ensure that the rules do not remain merely on paper, it is recommended to:

Tighten the monitoring mechanism. Member states need to regularly submit progress reports based on clear criteria such as their preparedness for cyber incidents, the number of expert personnel they have, and the extent to which they implement security rules. The Commission should review these reports to identify vulnerabilities or delays early and compel those countries to take action.

Provide targeted technical and financial support. EU budget and aid should be channelled especially to small businesses and public institutions with limited resources. Establishing common cybersecurity infrastructures for these institutions, providing expert training, and offering practical guides explaining the technical aspects will significantly facilitate their compliance, including the acquisition of secure servers that use local software.

Increase cooperation between countries. Member states should not only conduct joint cyberattack exercises, but also regularly share threat intelligence with each other in real time, and establish clear protocols on who will request assistance from whom, and how, in a major crisis. ENISA should act as a bridge here, organising these joint activities and ensuring the dissemination of best practices among countries.

These steps are not designed to discard the existing NIS2 rules, but to fill in their gaps. The main goal is to close the implementation gaps between countries and companies and to ensure that legal obligations are not merely symbolic but translate into real and measurable protection in the field.

Conclusion

The European Union has created a truly solid legal framework on paper in the field of cybersecurity. However, how effective this system will be depends entirely on how successfully the rules are implemented in practice. The disparity in the technical capabilities of countries, the shortage of expert personnel in the market, and limited budgets prevent the same efficiency from being achieved everywhere. The EU therefore needs to focus on supporting the full implementation of existing rules instead of constantly issuing new laws and directives. If stricter control mechanisms are established, targeted financial and technical support is provided to institutions with insufficient budgets, and inter-country cooperation is genuinely increased, the NIS2 Directive will not remain on paper; it will become a real and powerful cyber shield protecting us all.

References

1. European Commission. (2025, May 7). *Commission calls on 19 Member States to fully transpose the NIS2 Directive.* https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive

2. European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).* Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

3. European Union Agency for Cybersecurity (ENISA). (2025). *NIS Investments 2025.* https://www.enisa.europa.eu/publications/nis-investments-2025

Author: Sümeyye Cerit 2023173039

European Commission Policy Advisor

The content of this policy brief lies entirely with the author. It does not reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any organisers may be held responsible for the use which may be made of the information contained therein.