nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

2026 LUXEMBOURG GRC SUMMIT
powered by NC3

HOW CAN CYBERSECURITY CAPACITY AND COMPETENCE BUILDING IN EUROPE BE IMPROVED OR ACCELERATED?

OUTCOME PAPER

Key insights from the Luxembourg GRC Summit 2026 forum session on European cybersecurity capacity building, exploring possible improvements to market conditions, collaboration, funding, and talent development.

Table of contents

3	Summary
4	European Cybersecurity Capacity: Beyond Skills and Technology
4	Addressing Barriers in the European Cybersecurity Market
6	Connecting Europe's Cybersecurity Capabilities
7	Building Accessible and Impact-Oriented Funding Instruments
8	Building and Retaining Cybersecurity Capacity
9	Key Takeaways
10	Recommendations and Action Points

HOW CAN CYBERSECURITY CAPACITY AND COMPETENCE BUILDING IN EUROPE BE IMPROVED OR ACCELERATED?

Summary

This outcome paper provides a summary of the discussions that took place during the forum "How can cybersecurity capacity and competence building in Europe be improved or accelerated?", held as part of the second edition of the Luxembourg GRC Summit on 3rd and 4th June 2026. The Summit brought together Cybersecurity Governance, Risk and Compliance (GRC) professionals, practitioners and decision-makers to exchange knowledge, examine emerging threats, and explore evolving practices in the field.

Participants approached capacity building as a challenge covering skills, technology, governance, research, regulation and market development. The discussion focused on connecting Europe's existing capabilities, improving market access and funding, and creating conditions for innovation, talent and companies to develop and remain in Europe. The discussion converged on the need for stronger links across the ecosystem to achieve lasting European cybersecurity sovereignty.

European Cybersecurity Capacity: Beyond Skills and Technology

01

Cybersecurity capacity building cannot be reduced to increasing technical expertise or addressing the skills gap. The forum approached it as a broader challenge covering technical capabilities, governance, regulation, skills development, research and the conditions needed for cybersecurity solutions to reach the market. The aim is not only to strengthen Europe's ability to develop knowledge and technology, but also to translate these assets into products, services and capabilities that can be used across Europe, thereby creating and expanding market opportunities.

This reflects a broader evolution of the cybersecurity debate. As the ecosystem matures, questions of competitiveness, market development and European digital autonomy are becoming increasingly relevant. Europe already has significant expertise, research capacity and public investment, but these do not automatically translate into stronger companies, wider market adoption or a better functioning common market for cybersecurity solutions.

Making up about 99.8% of all businesses in the European Union,[1] SMEs are particularly relevant to this discussion, both as providers of cybersecurity solutions and as users that need access to appropriate products and services. Their ability to develop, adopt and scale cybersecurity solutions is therefore closely connected to the wider question of European capacity building.

Addressing Barriers in the European Cybersecurity Market

02

The forum identified structural weaknesses in the European cybersecurity market, emphasising that the problem involves more than just a shortage of European-made products. Participants pointed out distinct challenges on both sides of the market. On the supply side, providers face limited market visibility, strict barriers to entry and affordability constraints. On the demand side, customers struggle to find tailored solutions that offer adequate

[1] Annual report on European SMEs 2024/2025 - Publications Office of the EU. Available at: https://op.europa.eu/en/publication-detail/-/publication/2073ad00-3521-11f0-8a44-01aa75ed71a1/language-en

trust and ongoing support. SMEs are hit the hardest by these gaps: smaller buyers struggle to find suitable, budget-friendly cybersecurity solutions, while smaller vendors face uphill battles trying to connect with customers and scale past their domestic borders.

2.1. Reducing Market Fragmentation

Fragmentation remains a major obstacle to the European cybersecurity market. Despite the Single Market, cybersecurity products and services do not circulate easily across Member States, and organisations often favour domestic providers or established non-European suppliers.

Participants described cybersecurity as a trust-based market, where organisations need confidence in providers entrusted with sensitive data, systems and infrastructure. This can contribute to non-technical biases in supplier selection, including preferences related to a company's size or nationality.

Reducing national barriers and making providers accessible across borders are therefore insufficient on their own. Organisations need to identify and compare European solutions, while customer references, relationships and practical cooperation can help build confidence in unfamiliar providers.

Digital platforms can facilitate connections, but cannot replace these trust-building mechanisms.

The forum also highlighted a cultural dimension: overcoming domestic purchasing preferences requires European actors to see one another as parts of a shared ecosystem rather than competing national markets.

Combining national strengths with greater cross-border trust and cooperation would help Europe operate more effectively as a single cybersecurity market.

2.2. Public Procurement as Both a Driver and a Barrier

The forum suggested that public procurement could help strengthen the demand for European cybersecurity solutions. Public administrations represent a significant part of the market. By acting as early customers, public authorities could provide references, validate European solutions, and help European providers scale.

However, procurement procedures can also create barriers for smaller companies. One participating SME mentioned facing additional contractual layers when a public customer wished to expand an initial limited purchase. This illustrates how public procurement is not always realistically accessible to smaller providers.

Simplifying procedures and reducing unnecessary entry barriers could therefore make public-sector demand a more effective capacity building tool.

2.3. Preventing Unintended Market Effects of Compliance

Participants warned that complex or misunderstood compliance requirements may disadvantage smaller European suppliers that have fewer resources to demonstrate compliance. Customers may turn to larger providers, including non-European companies, perceived as easier or safer to contract with.

While regulation can strengthen cybersecurity demand, its implementation should avoid unintentionally reducing the diversity of the European supplier base.

Connecting Europe's Cybersecurity Capabilities 03

Europe already has significant cybersecurity expertise, research, companies and public support mechanisms. Participants identified three priorities for connecting European capabilities: matching solutions to customer needs, translating research into commercial applications, and improving cooperation and visibility across the ecosystem.

3.1. Bridging the Gap Between Demand and Supply

Participants questioned whether market weaknesses stem from insufficient supply alone. Cybersecurity is often treated as an add-on to broader IT projects rather than a dedicated investment, limiting demand and suppliers' incentives to develop specialised services.

Stimulating demand starts with a cybersecurity culture and shared responsibility among SMEs: businesses need enough awareness to understand their exposure, recognise their responsibilities and ask the right questions, while their ICT providers need adequate cybersecurity capabilities. Trusted intermediaries can help SMEs clarify their needs, translate them into requirements and assess suitable providers. Certification and labels can support this assessment, but cannot replace basic awareness.

Financial incentives such as cascade funding and public subsidies can lower initial purchasing barriers. Moreover, regulatory requirements such as those introduced through NIS2 can also encourage investment in cybersecurity and supply chain security, despite the perceived compliance burden.

3.2. Bridging Academia and Industry

Another major gap lies between research and commercial adoption. Participants noted that Europe produces strong research and intellectual property, but

often struggles to translate these into commercially viable cybersecurity products. Despite substantial European support, funding remains part of this problem. European instruments provide significant support for research and early-stage innovation, but participants described a severe shortage of investors and growth capital to help companies scale, leaving promising research without a clear route to market.

The challenge is therefore not only to finance research, but also to support valorisation, commercialisation and growth as technologies move beyond the research environment.

3.3. Increasing Visibility Across the European Ecosystem

Limited visibility of other actors' technologies and expertise can lead European organisations to duplicate work and miss opportunities for collaboration. Better information sharing can help identify partners developing comparable solutions or expertise. Stronger collaboration mechanisms could also help combine national and regional specialisations into shared European capabilities, rather than each Member State developing the entire value chain independently.

The ECCC's ATLAS platform was presented as a common entry point to European cybersecurity capabilities, aiming to connect organisations, help them identify potential partners, providers and technologies, and increase the visibility of funded projects and their results.

Building Accessible and Impact-Oriented Funding Instruments

04

Established in 2021 under Regulation (EU) 2021/887, the European Cybersecurity Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs) aim to strengthen the EU's cybersecurity capacity and technological autonomy through funding, strategic coordination and networking. Support includes European-level funding through the Digital Europe Programme (DEP) and Horizon Europe, as well as cascade funding delivered nationally through the NCCs. Participants questioned whether current funding instruments are sufficiently accessible, flexible and impact-oriented.

Smaller organisations can face difficulties accessing European funding because application and reporting processes are often complex and resource-intensive.

The fragmentation of the European funding landscape adds another layer of difficulty: participants may struggle to even identify the most appropriate funding channel. Participants called for simpler procedures and clearer information on available funding opportunities.

4.1. Increasing Risk Tolerance and Funding Flexibility

Participants also called for greater flexibility in the way cybersecurity innovation is funded. European programmes were described as highly structured, with extensive application and reporting requirements and limited room to depart from the original project plan. This can be difficult to reconcile with innovation, where assumptions, technologies and opportunities might change during implementation.

The forum discussed possible solutions such as mixed public-private funding, public funds absorbing part of strategic investment risk, and proactive support for promising companies alongside traditional calls. Adjusting funding rates to support more projects was also suggested.

4.2. Turning Funding Into Wider Ecosystem Impact

The ECCC and the Network of NCCs already support a large number of cybersecurity projects through direct and cascading funding. The question raised during the forum was how to ensure that the results, knowledge and technologies generated by these projects circulate beyond the individual beneficiaries and create wider European impact.

Cascading funding was highlighted as particularly useful because it injects funds directly at the core of national ecosystems, supporting implementation and market uptake while helping smaller companies develop and scale.

To extend these benefits beyond individual recipients, funding should be accompanied by mechanisms for disseminating, identifying and reusing project results. Success should reflect their contribution to stronger companies, new solutions and shared capabilities, alongside project delivery.

Building and Retaining Cybersecurity Capacity

05

Because educating new professionals takes time, participants stressed the need to combine long-term skills development with immediate reskilling and upskilling of existing employees. Proposed approaches included cooperation between universities, student mobility, and university-

business partnerships enabling employees to combine work and study. ENISA's European Cybersecurity Skills Framework can support workforce planning, skills gap analysis and training design, helping align learning with operational needs across the EU.

Creating skills and supporting innovation is not enough if the resulting capacity leaves Europe. Participants highlighted the difficulty of retaining both cybersecurity professionals and growing companies when better salaries, larger markets, greater risk tolerance or more accessible financing are available elsewhere. Europe can therefore invest in education and innovation and still lose part of the capacity at the scale-up stage.

Buying European solutions alone cannot secure lasting autonomy if companies subsequently relocate or come under non-European ownership. Retaining and developing capabilities requires access to talent, research and innovation, growth capital, cross-border markets and sustained demand for European solutions. The forum consequently pointed towards a combination of measures that need to work together rather than a single solution.

Key Takeaways

The forum showed that European cybersecurity capacity building is not simply a matter of funding more projects or training more professionals. Europe already has substantial expertise, research capability, companies and public investment. The main challenge is to connect these assets more effectively so that they translate into stronger providers, accessible services, functioning cross-border markets, and capabilities that scale across the EU. As one participant summarised it, ***Europe needs to become more effective as a system, not only excellent in individual areas.***

This requires action across the whole ecosystem. SMEs need awareness, practical support, trusted intermediaries and accessible funding rather than being expected to develop specialised cybersecurity expertise internally. Providers need stronger demand, easier access to public procurement and funding, and better opportunities to grow across borders. Research and innovation also need clearer paths towards commercialisation, while skills development must be combined with better conditions for retaining talent and companies in Europe.

The overall approach must therefore remain systemic: research, valorisation, funding, skills, market conditions, public procurement, demand and cross-border cooperation all contribute to sustainable

European cybersecurity capacity. Local and national ecosystems remain important starting points, but these ecosystems need to connect progressively at European level.

Strategic autonomy will depend less on a single policy measure than on Europe's ability to turn existing capacity into scale, impact and lasting market presence.

Recommendations and Action Points

01. Strengthen the **connection between cybersecurity demand and supply.** Support mechanisms that help organisations, particularly **SMEs**, clarify their needs and identify suitable providers.

02. Use public procurement to support market uptake. Simplify procedures and reduce unnecessary entry barriers to smaller providers.

03. Make **cybersecurity funding** easier for SMEs to access. **Simplify application processes**, improve **visibility** of available instruments and reduce unnecessary administrative burden.

04. Introduce **more flexible and risk-tolerant funding**. Allow projects to adapt during implementation, **use public-private risk-sharing**, and complement traditional calls with **proactive support** for promising companies and technologies.

05. Measure funding success through ecosystem impact, not only project delivery. Create mechanisms to ensure the **knowledge, technologies and solutions** generated through public funding are shared, reused and made visible.

06. Strengthen pathways from research to market. Support closer cooperation between academia and industry and programmes specifically designed to turn research results into deployable solutions.

07. Combine education with professional skills development. Support reskilling, university-business partnerships, student mobility and models combining employment with further education.

08. Improve visibility of European cybersecurity capabilities. Develop and strengthen **mechanisms and tools** such as ATLAS, national catalogues, networking initiatives and community events to **connect stakeholders.**

09. **Build cross-border cooperation around complementary strengths.** Identify national and regional areas of cybersecurity specialisation and connect them at European level to reduce duplication.

10. Support the retention and growth of European talent and companies through access to growth capital, cross-border market opportunities and attractive career conditions.

Thank you for reading. We hope these insights inform your work and encourage further dialogue on cybersecurity governance.

Thank you to our participants, Advisory Board and partners for sharing their expertise, **and to you for taking these discussions forward.**

nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

IN COLLABORATION WITH

Luxembourg House of Cybersecurity

LUXEMBOURG CYBERSECURITY FACTORY