The European Path Toward Cyber Resilience

Insights from Forum InCyber 2026

Nanbaan Pwaspo (CII Young Talent Program)

Cyber resilience is no longer a peripheral concept in Europe's cybersecurity landscape; it is rapidly becoming its organising principle. At the recently concluded Forum InCyber, there were many discussions about how Europe is gradually moving beyond prevention to preparedness and coordinated response. From sovereignty, Law and regulation to emerging technologies such as AI, discussions highlighted the new and proposed strategies of Europe's cyber defense and recovery capabilities. It is also worth noting that there remains a gap between our ambition and the operational realities faced by many organizations and institutions today.

Some of the discussions highlighted how "resilience" is strongly tied to Europe's goal of reducing dependencies and increasing our control over our technological ecosystem. Initiatives such as Cyber ranges, simulation environments, and well-coordinated training platforms are also positioned as essential for building operational readiness.

The strategic value of the ongoing dialogue with Business France was validated by the Institute's presence at the Forum. Enabled by this partnership, our participation allowed for a direct assessment of how the French cyber-startup ecosystem can be integrated into German and European dialogue formats.

This is a practical investment in the German-French Cyber-Ecosystem, moving us toward a unified European register where we "think European from the beginning." This philosophy is the core of the **EUCRA (European Value Alliance for Cybersecurity and Resilience**) initiative, bringing French startup innovation and German strategic dialogue together to build a truly "European-first" mindset. By baking sovereignty into the development phase of our digital infrastructure, we avoid the need to retrofit security as a response to external dependencies.

Sovereignty and Regulation as Factors Building Resilience

Throughout the Forum, one question kept coming up: Is Europe still too dependent on outside technology? Whether it's our cloud infrastructure or core software, there is a growing concern that we are "renting" our digital future rather than owning it. This theme ran through every debate about supply chain security and the push for SBOMs. Ideally, sovereignty should give us the visibility and control to manage our own risks at scale.

The core premise of the EUCRA initiative is to 'think European from the very beginning.' This shift in mindset ensures that sovereignty is baked into the development phase of our digital infrastructure, rather than being retrofitted as a response to external dependencies

Regulatory frameworks such as NIS2 and the Cyber Resilience Act are central to this, not only setting baseline requirements but actively shaping how organisations design and manage their systems. However, this growing regulatory pressure also risks prioritising compliance over capability, particularly for organisations with limited resources.

The Reality Gap

Cyber resilience conversations have since advanced. However, implementation has not kept pace.

Many of the approaches, like advanced cyber ranges and automated security tools, assume a level of maturity that some organizations have not yet reached. Teams are still battling with legacy systems, tight budgets, and small team capacity. And when we add the weight of new regulations like NIS2 or the Cyber Resilience Act, there is a threat that under-resourced teams will end up focused on checking boxes rather than actually enhancing security.

Perhaps we also should ask who we are leaving behind. The focus was largely on critical infrastructure and big business, with limited attention given to at-risk groups. If resilience frameworks do not include these high-risk communities, then we cannot call them comprehensive. To bridge this gap, we have to start building adaptable, inclusive strategies.

Key Strategic Developments

1. **AI and the Shift Towards Autonomous Defense**

   AI has shifted from a standalone feature to the central part of modern security infrastructure. The industry is adopting Autonomous Defense systems that can self-heal and reconfigure networks in real-time. Since the OODA loop (Observe, Orient, Decide, Act) now functions at machine speed, any defensive approach depending on manual human intervention is gradually becoming outdated.

2. **The Cyber-Physical Measure of Resilience**

   Under the 2026 theme of Mastering Dependencies, the focus has moved from theoretical to practical Operational Continuity. This is vital for the Cyber-Physical bridge, where the success of a strategy is no longer measured by the number of incidents prevented, but by the ability to maintain essential services and minimize downtime during a sustained attack.

3. **Post-Quantum Readiness as an Immediate Priority**

   Post-Quantum Cryptography (PQC) is now a current migration requirement. As standards are now integrated into core vendor products, the focus has shifted to the "migration nightmare" of updating legacy systems. Organizations that have not yet initiated a PQC inventory are facing a decade-long strategic liability that starts today.

4. **Regulation as a Driver of Competitive Advantage**

   There is a clear shift in how frameworks like NIS2 and the Cyber Resilience Act (CRA) are perceived. Instead of being viewed as administrative "red tape," these regulations are being utilized as a competitive advantage. By adhering to these high European standards, organizations are exporting security values and establishing "EU Compliance" as a global gold standard for trust.

5. **Cognitive Threats and the Expanding Security Perimeter**

   Perhaps the most significant (and darkest) theme of 2026 is the rise of Cognitive Warfare. We are seeing that you don't need to breach a server if you can successfully "hack" the person operating it. As deepfakes become indistinguishable from reality, the definition of

security is expanding. The challenge is no longer just protecting the server, but protecting the integrity of the information consumed by the user.

A Call to Action for European Stakeholders

To build a truly resilient ecosystem, we recommend:

1. **Operationalizing the EUCRA:** Transition the European Value Alliance from a policy framework into a practical "Register of Trust" for vetted, sovereign value chains.
2. **Bridging the Resource Gap:** Develop “Resilience-as-a-Service” models to support under-resourced sectors navigating increasing regulatory and operational demands.
3. **Prioritizing Information Integrity:** Integrate cognitive defence into standard security architectures, recognising that protecting the integrity of information is as critical as securing the systems that host it.

Conclusion

Cyber resilience is no longer merely a defensive requirement; it is a fundamental pillar of European economic strength. By securing our value chains, we are protecting the competitive edge of the Union’s industrial base.

Europe has the talent, the frameworks, and the ambition to lead in cyber resilience. The challenge now is execution. The most vital lesson from this year is that building is not the same as acting. We have exceptional talent and institutions building solutions for resilience, but that architecture remains unfinished as long as it stays confined to the 'sandbox.'

The path forward demands that we be as pragmatic as we are ambitious. We must ensure our frameworks don't just look good on paper. By turning these strategic ambitions into an inclusive, operational reality, we move beyond 'renting' our security from others. We begin to take ownership of it ourselves.