THE POLICY SIGNAL

The 13th Annual European Cyber Security Conference

The rules are largely in place: NIS2 is in implementation and the Cyber Resilience Act applies in full from December 2027. The conference asked whether the capacity behind them, to patch, to replace suspect suppliers and to share threat information across borders, can keep pace now that AI is accelerating the discovery of flaws.

FORUM EUROPE • BRUSSELS • 4 NOVEMBER 2026

IN THIS ISSUE

01 The Signals · eight readings
02 The Briefing · four sections
03 What happens next
04 What's next at Forum Europe · About

THE POLICY SIGNAL

The **Signals**

MOMENTUM

01 Basic controls required under NIS2 address the legacy weaknesses behind recent incidents

Speakers traced recent incidents to unsupported systems, default credentials and unmanaged devices, which AI-assisted attackers can now find faster. Asset inventories, two-factor authentication, patching and restricted access were put forward as the answer. Whether they will hold against future AI capability was left open.

MOMENTUM

02 AI-assisted discovery is moving the bottleneck to testing and patch deployment

As discovery volumes rise, prioritising repairs gained weight in the discussion. Finding flaws is getting cheaper. Testing and deploying fixes still takes engineering time.

WATCH

03 CSA2 has not settled how high-risk suppliers are designated, how fast they are replaced or whether certification becomes mandatory

CSA2, the proposed revision of the Cybersecurity Act, exists in drafts that differ over country-based checks and company designation; the Council's text combines both. One camp wanted trust to rest on harmonised technical security practice. The other held that extra-legal control of a supplier cannot be tested, and requires an assessment of jurisdiction and judicial redress. Rapid replacement of high-risk equipment had support, but its pace did not: some argued the proposed 24-month phase-out for mobile networks is too long and voluntary certification too slow, while others countered that contracts already drive established standards and that deadlines must reflect risk, equipment value, service continuity and funding.

MOMENTUM

04 Scarce growth capital and 27 national markets hold back European cybersecurity firms

Early-stage funding is available; scale-up capital often comes from outside Europe. The proposed European Competitiveness Fund would broaden financing beyond grants, but depends on negotiation of the next EU long-term budget.

WATCH

05 Reducing critical dependencies leaves a role for international technology partnerships

Strategic autonomy was framed as having trusted alternatives and keeping services running if a supplier becomes a risk, without cutting access to allied technology. Advocates of European cloud partnerships offered jurisdictional safeguards, key control and continuity. Sceptics replied that geopolitical dependencies can still threaten essential services, and that Europe needs more alternatives of its own.

THE SIGNALS · CONTINUED

MOMENTUM

06 Cross-border incident sharing depends on knowing how reported information will be used

Trust, reciprocity and respect for handling restrictions were described as what moves sharing beyond legal minimums. Separating assistance from enforcement was proposed to encourage it. A draft incident taxonomy aims to align technical and operational crisis work.

WATCH

07 ENISA has backing for a stronger operational role; its testing role is contested

Support extended to more staff, funding and member-state presence at the agency. Proposed amendments to CSA2 would add compute, a testing environment and a single entry point for assistance. Whether ENISA has the expertise for testing, and whether it would duplicate allied work, remained in dispute.

WATCH

08 Defenders' access to advanced AI, and the agents they deploy, both need rules the EU is still writing

The July 2026 Action Plan on Cybersecurity and AI provides for a blueprint on structured access to cyber-capable models. Objective eligibility criteria were proposed to support European access and clarify security expectations, against calls for critical defenders to get early access to diverse tools. Agents holding network credentials can become a target or an insider risk, and need identity, privilege and monitoring controls of their own.

Momentum marks a direction supported across independent parts of the discussion. Watch marks a point that remained contested, under-evidenced or dependent on a future decision.

THE BRIEFING · 01

Operational resilience and remediation

Recent large incidents, speakers argued, were not sophisticated. They exploited unsupported systems, default credentials and unmanaged devices: the basic weaknesses that NIS2's risk-management duties, now binding on operators in 18 sectors, were written to remove. The Cyber Resilience Act adds lifecycle requirements for products from December 2027.

Transposition of NIS2 remains incomplete and implementation uneven. Attacks on supermarket refrigeration systems were cited to show that retail, which falls largely outside NIS2's scope, is exposed all the same.

Operational technology has drawn sustained attacker interest. Asset inventories, two-factor authentication, restricted access and network separation reduce exposure. Speakers presented these measures as buying defenders time. Whether they suffice against future AI is unknown.

NIS2 places accountability for these measures on management bodies. One proposal went further: the security chief should report directly to the head of the organisation and coordinate HR, IT and physical access.

Measurement drew similar attention. Speakers called for continuous maturity assessment scaled to organisation size, and for awareness work aimed at privileged IT administrators and executive assistants. Staff risks include malicious links and personal data entered into public AI tools.

AI-assisted analysis is increasing the number of vulnerabilities found. Repair has not kept pace. Each fix still needs testing, deployment and engineering time, and open-source maintenance gaps and costs make prioritising remediation both more necessary and harder.

A keynote speaker argued that shielding vulnerable code can limit exposure, citing the rapid patching of a PHP flaw that helped governments and major companies avoid a widespread incident. The flaw was hard to exploit, which left time to patch.

Migration to post-quantum cryptography was placed within the same legacy modernisation effort.

THE BRIEFING · 02

Supplier assurance and European capacity

How the EU should decide which technology suppliers are high-risk is unresolved. CSA2 would allow EU-level restrictions, and the Council's text combines country checks with company designation. Naming firms rather than countries was put forward as a way to avoid country-list decisions while still addressing the law of a supplier's home jurisdiction and access to judicial redress.

The dispute was over what kind of risk this is. One camp treated ownership, control and jurisdiction as non-technical risk requiring jurisdictional checks, not product certification. The other wanted trust to rest on harmonised technical criteria from production to patching, wherever a supplier is headquartered, with product and sector risk indicators rather than geography determining restrictions.

Supply chains complicate country restrictions. Some speakers warned that they could hold back European ICT supply chains, since components cross jurisdictions. Others replied that Title IV of CSA2 concerns non-technical control of direct suppliers, not whole component chains, and that national-security restrictions are needed even where realistic alternatives are few. Latvian law already excludes Russian and Belarusian products from critical infrastructure.

Rapid replacement of high-risk equipment had support; the argument was over pace. Strict timelines, some warned, could overwhelm smaller firms without explicit funding. Others noted that the proposed phase-out concerns mobile networks, where operators have switched vendors within normal investment cycles. The Council's text would let deadlines reflect risk, equipment value and service continuity.

Certification divided the discussion along similar lines. Those favouring mandatory certification in some cases pointed to an EU framework that has delivered few schemes and little uptake, and to organisations' resistance to voluntary process change. Opponents warned that unfamiliar mandatory schemes would raise costs, and that customer contracts already drive adoption of established standards.

Political-risk concern is delaying cloud upgrades. European cloud partnerships were offered as the answer, combining jurisdictional safeguards, key control and continuity. Sceptics held that geopolitical dependencies can still threaten essential services, and that the answer is more European alternatives. Speakers also called for a binding EU-UK digital partnership to clarify cloud and satellite eligibility, and for public-private cooperation on monitoring and repairing subsea cables.

THE BRIEFING · CONTINUED

Speakers identified growth capital as the main constraint on European firms. Early-stage money exists, but scale-up capital often comes from abroad, and 27 sets of national rules complicate expansion. The proposed European Competitiveness Fund would move financing beyond grants, and depends on negotiation of the next long-term budget.

Procurement was the other lever discussed. Speakers wanted it to reduce import dependence and widen opportunities for European firms, while keeping European providers that use international partner technology eligible. Common standards could help smaller firms demonstrate their security.

Suppliers outside NIS2's legal scope will meet its requirements anyway, through their customers' contracts. Speakers described skills shortages as constraining growth, with trained staff lost to recruitment abroad; others insisted that European expertise remains strong.

THE BRIEFING · 03

Shared intelligence and crisis coordination

The machinery for cross-border crisis response exists. The question raised was whether information survives the journey through it. Under the 2025 EU Cybersecurity Blueprint, national response teams exchange technical indicators and EU-CyCLONe (the network of national cyber crisis authorities) assesses impact. The EU Cybersecurity Reserve, under the Cyber Solidarity Act, can supply response services, and decisions on political escalation and reserve activation draw on an EU-wide picture.

Without a clear interoperability framework, speakers warned, information can be lost between technical, operational and political levels. EU-CyCLONe is drafting an incident taxonomy combining technical and operational impact levels. It will not be mandatory.

ENSOC, a cross-border hub linking security operations centres in eight countries, has moved from approved funding into procurement, deployment and integration.

Voluntary sharing rests on trust. Reciprocity and respect for handling restrictions encourage it, and separating assistance from enforcement was proposed as a further incentive. Views split on entry points: common European ones would reduce fragmentation, against the view that confidence rests on national relationships built over years. Belgian practice was cited, where an initial notification within 24 hours can bring assistance before an investigation is complete.

THE BRIEFING · CONTINUED

AI could convert incompatible intelligence formats into a common one, provided the output is checked against the original reports. Sharing also needs legal support, and engineering staff beyond those covering incidents.

Sharing between government bodies faces political barriers. Others replied that NIS2 already imposes cooperation duties on those bodies. A directly applicable regulation, rather than a directive, was proposed as a way to reduce national differences in reporting.

CSA2 would revise ENISA's mandate, and there was support for more staff and crisis-response funding. Proposed amendments would add computing capacity, AI testing and a single entry point for assistance; ENISA is already testing AI models and developing containment and human-oversight guidance. The testing role divided opinion. Sceptics questioned whether ENISA has the expertise and resources, and whether it would duplicate allied work. Supporters argued that Europe needs testing capacity of its own.

THE BRIEFING · 04

AI access and governance

Most defensive work, speakers noted, does not need frontier systems. Open-weight models and specialist tools offer alternatives. The July 2026 Action Plan on Cybersecurity and AI provides for a structured-access blueprint, and its terms were contested: supporters of objective eligibility criteria argued they would support European access and clarify security expectations, while others pressed for critical defenders to get early access to a diverse range of tools.

The AI Act already applies to the largest models. Providers of general-purpose models with systemic risk have had to assess and mitigate those risks since August 2025, and the AI Office can enforce those duties from August 2026.

A frontier-model developer pointed to withheld releases, paused testing after incidents, alignment training, containment and monitoring as evidence that safety precautions are real. Others countered that security by default should have been designed in from the start, to prevent avoidable faulty outputs.

Agents deployed by companies and governments need controls of their own. An agent holding network credentials can become a target or an insider risk, and needs its own identity, restricted privileges, monitoring and human oversight. These measures complement the risk assessment the AI Act requires of model providers.

THE BRIEFING · CONTINUED

Speakers suggested that European models can run a few months behind the frontier, and that training-data provenance, not only country of origin, should inform assessment. Closer links between AI specialists, cyber agencies and smaller critical operators were called for.

Beyond the EU, common definitions of frontier capability and incident severity were proposed as a basis for international AI governance, with the EU framework and code of practice offered as models. Attribution and coordinated sanctions were urged against state-linked hybrid campaigns, and offensive options were raised for consideration.

LOOKING AHEAD

What happens next

Decision points and dates recorded in the discussion

Since 11 September 2026

The Cyber Resilience Act's reporting obligations apply, including to in-scope products already on the market.

Under way

The AI Office has sent formal information requests on model security and on external evaluators' pre-release access, independence and freedom to publish.

From December 2026

The first European standards supporting the Cyber Resilience Act are expected, subject to approval by national standardisation bodies.

By end of 2026

The Commission and ENISA aim to complete revised Situation Centre operating procedures.

In draft

EU-CyCLONe's incident taxonomy. Whether it will be published is undecided.

Planned

The structured-access blueprint under the July 2026 Action Plan on Cybersecurity and AI, and a grand challenge for market-ready European AI cyber tools.

2027

Lithuania's Council presidency is due to take forward the pending CSA2 and NIS2 amendments.

Next long-term budget

The proposed European Competitiveness Fund depends on negotiation of the next Multiannual Financial Framework.

11 December 2027

The Cyber Resilience Act's main product requirements apply.

FORUM EUROPE · FORUM GLOBAL

What's next at Forum Europe and **Forum Global**

2026		
17 November 2026	European Accessibility Summit 2026	Brussels, Belgium
30 November–1 December 2026	The Americas Space Forum 2026	Santiago, Chile
2 December 2026	The International AI Summit 2026	Brussels, Belgium
7–8 December 2026	15th Americas Spectrum Management Conference	Washington DC
9 December 2026	The Americas D2D Policy Forum	Washington DC
2027		
Q1 2027	3rd Caribbean Spectrum Management Conference	Miami
28 January 2027	AI Britain Summit 2027	London, United Kingdom
28 January 2027	The Child Safety Online Conference 2027	Brussels, Belgium
Late January or early February 2027	10th MENA Spectrum Management Conference	Egypt
3–4 February 2027	Masters of Digital 2027	Brussels and Online
4 February 2027	Financing Europe 2027	Brussels
17–18 February 2027	ECS Brokerage 2027	Brussels, Belgium
Q1–Q2 2027	Quantum Europe 2027	Brussels, Belgium

EVENTS **Forum Europe events** · forum-europe.com

WHAT'S NEXT · CONTINUED

ABOUT

The Policy Signal is an independent editorial synthesis of the 13th Annual European Cyber Security Conference, produced by Forum Europe. It reads the policy temperature of the event for those who were there and those tracking the direction from a distance, recording the positions taken and the points left unresolved, in aggregate and without attribution.

This synthesis was based on AI-assisted transcription and should be verified against official sources before reliance.

Disclaimer: This Signal is provided for general information only and does not constitute legal, investment or policy advice. While reasonable care has been taken, Forum Europe accepts no responsibility or liability for any loss or damage arising from reliance on it. Positions and figures are recorded in aggregate and are not findings of Forum Europe.