EVENT REPORT

HIGH-LEVEL CONFERENCE 2025

STRATEGIC AUTONOMY IN ACTION:

Keeping Europe and its Borders Secure with Trusted Technology

1 OCTOBER 2025
TALLINN / ESTONIA
& ONLINE

eu-LISA

CONTENTS

eu-LISA

EU-LISA HIGH-LEVEL CONFERENCE EXECUTIVE SUMMARY 1st OCTOBER 2025

On 1 October 2025, eu-LISA held in Tallinn, Estonia, and online, its annual High-Level Conference on "Strategic Autonomy in Action: Keeping Europe and its Borders Secure with Trusted Technology" attended by approximately 300 senior stakeholders from the national authorities, EU institutions, industry and academia.

Key topics relating to technological sovereignty of critical systems, rule of law and digital skills for strategic autonomy were discussed in the margins of the launch of the Entry/Exit System (EES) on 12 October 2025, as the first operational step toward building the technological and decision-making foundations of European sovereignty.

Throughout the event, a shared set of strategic challenges was identified relating to the current questions that Europe is facing in the technological domain. These included technological dependency, evolving security aspects, complex legal frameworks and procurement rules, and persistent gaps in attracting, training and retaining skilled professionals.

As far as opportunities are concerned, these arise from strong political will to lead in technology, broad trust in the European values, and increasing public awareness. Proposed solutions focused on reducing the dependence on external suppliers while promoting local industry as well as "thinking and buying European". The need to harmonise and simplify regulatory processes, accelerate decision-making and ensure consistency across Member States was also stressed. Expanding and funding educational programs was also identified as essential in boosting the attractiveness and competitiveness of the European technology sector. Additionally, the importance of interoperability and information sharing, balanced with EU values and technical realism, was underlined throughout the discussions.

Main takeaways highlighted that policy, and policymaking should be informed by technological understanding and backed by long-tern commitment. Combined with excellent governance, clear objectives, efficient regulation, cooperation among Member States and industry, and robust investment in skills, research and talent, these measures are essential to advancing Europe's strategic autonomy.

The 2025 eu-LISA High-Level Conference, dedicated to the strategic role of sovereign technologies in keeping Europe and its borders secure, took place on 1 October 2025, in a hybrid format (Tallinn, Estonia and online).

The event provided a forum for discussions and debates at the intersection of technology, rule of law, and strategic skills development, delving into eu-LISA's role in the context of the EU's quest for strategic autonomy.

Austria • Belgium • Bulgaria • Croatia • Cyprus • Czech Republic • Denmark • Estonia • Finland • France • Germany • Greece • Hungary • Iceland • Italy • Latvia • Liechtenstein • Lithuania • Luxembourg • Malta • Moldova • Netherlands • Norway • Poland • Portugal • Romania • Slovakia • Slovenia • Sweden • Spain • Switzerland • United Kingdom • United States • European Commission • European Parliament • CEPOL • EDPS • EPPO • EUAA • eu-LISA • Eurojust • Europol • FRA • Frontex

22 speakers

34 countries

12k web views

95% satisfaction rate

OPENING REMARKS

MAGNUS BRUNNER

European Commissioner
for Home Affairs

„The EU has a unique opportunity to position itself on the frontier of new technology in the growing security economy"

European Commissioner for Home Affairs, **Magnus Brunner**, delivered a video address highlighting the challenges and opportunities of sovereign technologies. He stated that the operations of migrant smugglers and the trafficking of illegal drugs were putting the EU's borders and systems of aid under undue strain. Commissioner Brunner outlined that *"securing borders is a big challenge that will require not only significant resources, but also joint thinking by the private sector and government"*. But strategic autonomy is also an opportunity for the EU to lead in innovation within the growing security economy. Commissioner Brunner stressed that achieving this goal required excellent governance, clear rules, and defined objectives, asserting that with enough ambition, every challenge could become an opportunity. The audience of the eu-LISA High-Level Conference was invited by Commissioner Brunner to *"think big, think bold, and set sights high"*.

IGOR TARO

Estonian Minister of Interior

„The Entry/Exit System is not a single project but a piece of a larger plan for European security and technological independence."

Estonian Minister of the Interior **Igor Taro** emphasised that strategic autonomy extended beyond technology to include values and independence. He stated that Europe needed to ensure that its hardware and software were developed within the EU using its own knowledge to avoid dependency on foreign suppliers. Mr Taro highlighted Europe's shortage of skilled professionals for managing large cross-border technology projects. He called for a balance between independence and practicality *"without giving up our security or principles,"* stressing that autonomy required deliberate investment and strategic choices. The Minister concluded that strategic autonomy meant the ability to look at both the risks and opportunities while protecting Europe's values—freedom, security, and fundamental rights. *"Afterall"*, he stated, *"our task is to make wise choices in a complicated world."*

RENE VIHALEM

eu-LISA Management Board Chairperson

„The EU, its Member States, and eu-LISA, are like a family each concerned for the other."

Rene Vihalem, Chairperson of the eu-LISA Management Board, reflected on the relations between EU institutions and the EU Member States, highlighting the important role national authorities play in turning legislation into action. Mr Vihalem explained that eu-LISA played a key role in implementing IT systems that required new communication standards, often launching debates about possible technologies and solutions. On this, Mr Vihalem noted that *"there's an added value on many systems – but we always have to look inside the software and determine where that value will really take us."* Over time, Member States, including Estonia, recognised the benefits of these new solutions and began adopting them domestically. He described this process as constant negotiation and collaboration. Looking ahead, Mr Vihalem highlighted the increasing knowledge we gather on immigration, and the importance of future reflection on this topic, that will continue to influence the work of all relevant EU stakeholders.

MARILI MÄNNIK

eu-LISA Executive Director ad interim

„This conference is about how we, collectively, can ensure that Europe remains not isolated, collaborative with clear principles, resilient, secure, and future-ready."

Marili Männik, eu-LISA Executive Director ad-interim, stressed the importance of this year's conference main theme: strategic autonomy in action. Ms Männik highlighted that eu-LISA is currently at the full speed of implementing the new home and justice affairs systems, after having launched the Shared Biometric Matching System in May 2025 and with the imminent progressive entry into operation of the Entry/Exit System, on 12 October 2025. With the world changing at a rapid pace and emerging technologies transforming our societies, Ms Männik outlined the challenges for *"pursuing strategic autonomy and ensuring that we can deploy trusted technology to safeguard the EU, its Member States and its citizens."*

Ms Männik called for seeking opportunities to *"expand open-source software use, strengthen partnerships with strategic allies, and identify European champions that could potentially fill the technological gaps."* Ms Männik emphasised the importance of developing European cloud services to ensure data sovereignty and leveraging the public sector's demand to strengthen domestic providers. She as well underscored cybersecurity as a major vulnerability, urging investment in European cyber capabilities, trusted cloud and encryption solutions, and the secure storage of sensitive data within the EU.

Ms Männik concluded that the conference aimed to find practical solutions to ensure Europe remained collaborative yet sovereign and secure.

HIGH-LEVEL DEBATE ON DIGITAL SOVEREIGNTY

Moderator:
JOHANNES TRALLA
eu-LISA High-Level
Conference moderator

By launching a discussion around the concept of digital sovereignty at EU level and the way this could be considered when developing and implementing policies in the JHA area, the high-level debate set the scene for the subsequent panel discussions. During this debate the panellists explored ideas about the role of different stakeholders in contributing to EU's efforts to strengthen our borders, security and justice while aiming for leadership in the technology field.

Panellists:

TIINA UUDEBERG
Secretary General, Estonian Ministry of Justice and Digital Affairs

MARIA BOULIGARAKI
Head of the Programme and Engineering Department, eu-LISA

PHILIPPE VAN DAMME
Deputy-Director General, DG-DIGIT, European Commission

Mr Tralla opened the high-level debate on digital sovereignty by inviting the panellists to assess whether digital sovereignty was an achievable goal and what sovereignty means in practice.

Explaining DG DIGIT's approach, Mr Philippe Van Damme outlined how the Directorate pursued a pragmatic approach to digital sovereignty focused on operational control over the European Commission's extensive digital ecosystem of over 1,000 information systems and 43,000 users. He defined sovereignty through resilience, reduced dependence on proprietary software, supply chain diversity, avoidance of external strategic control, and interoperability. In Mr Van Damme's opinion, assessing *"what are the capabilities that we need to increase our technological autonomy without compromising our efficiency, business continuity, and budget"* should always be the priority when determining how to realize digital sovereignty.

Tiina Uudeberg stated that in democratic societies, justice must remain independent and trusted, and in the digital era this meant controlling data, infrastructure, and software. Estonia's approach, she said, relied on its secure X-Road data exchange

system, strong cybersecurity, distributed architecture, and the innovative "data embassy" concept for safeguarding national data abroad. She stressed resilience, preparedness for crises, and innovation as pillars of digital sovereignty while acknowledging dependence on non-European technologies. Noting that EU regulation sometimes hindered frontrunners like Estonia, citing difficulties aligning its X-Road platform with the EU's digital wallet system, Ms Uudeberg called for recognition that *"enabling innovation must be one of the prerequisites while drafting EU laws in order for the EU to be a global player in digital sovereignty."*

Ms Maria Bouligaraki described eu-LISA's reliance on non-EU technologies as inevitable given global markets and the need to deliver interoperable, large-scale IT systems for EU Member States. She noted that balancing cost-efficiency with security, resilience, and data protection was central to the agency's mission. She cited EU Parliament and EU Commission initiatives promoting both sovereignty and international cooperation and emphasised that Member States must trust eu-LISA with their data while striving for secure and compliant solutions.

On the topic of international partnerships, Philippe Van Damme promoted "open sovereignty," suggesting collaboration with partners sharing European values, both within and beyond Europe. He cited the example of negotiations with Microsoft that led to improved privacy compliance for Microsoft 365 as proof that cooperation could enhance European norms.

On balancing cost, speed, and control, Tiina Uudeberg admitted that Estonia prioritised time and security over cost, given its proximity to Russia, but still aimed to favour European and Estonian solutions. Ms Bouligaraki added that eu-LISA operated under strict deadlines and budgets, requiring practical trade-offs between efficiency and security.

Asked whether Europe should limit its digital ambitions, Philippe Van Damme rejected the idea, arguing for pragmatism and incremental progress rather than reduced vision. Citing the Commission's new "digital-ready" policy framework and efforts to raise digital literacy among policymakers, Mr Van Damme outlined that policy building should remain aspirational but that *"desirability must at the same time be balanced with a proper sense of reality."*

On shaping global digital standards, the panel cautioned against overregulation and excessive bureaucracy. The collective responsibility among EU institutions and companies to "buy European," fostering market-driven sovereignty was emphasized by Mr Van Damme who added that citizens need to think in European rather than national terms. Ms Uudeberg emphasised education and state leadership to build public understanding of digital sovereignty from an early age, while Ms Bouligaraki observed that citizens often appreciated sovereignty only after suffering data breaches or system failures.

Mr Van Damme illustrated interoperability's importance by contrasting a highly sovereign open-source website hosted on an American hyperscaler with proprietary on-premises systems dependent on costly vendor negotiations. Ms Bouligaraki added that strategic autonomy in infrastructure required transparency, traceability, and visibility across software and hardware systems.

As far as procurement guidelines are concerned, Mr Van Damme warned that digital sovereignty risked becoming over-politicised, arguing for measurable, objective frameworks. He described a forthcoming EU tender for a sovereign cloud that would evaluate all suppliers—European or not—against eight sovereignty criteria, from legal compliance to sustainability. Ms Bouligaraki stressed that *"procurement is a tool to help us deliver efficiently while also maintaining the boundaries for data protection security."* Thus, the need for flexible procurement that balanced efficiency with protection. Ms Uudeberg added that transparency was crucial to ensure safety and fairness in procurement.

Looking forward to European Digital Sovereignty by 2030, Mr Van Damme envisioned a Europe united by "European thinking," with open sovereignty, fewer proprietary systems, more open-source adoption, and fairer licensing models. Ms Bouligaraki envisioned a common European interoperability framework enabling secure cross-border data sharing without undermining sovereignty. Ms Uudeberg foresaw a common digital area where citizens were technologically educated, systems were interoperable and secure, and Europe held a strong position in the global IT ecosystem.

In closing, and as a goal for the next five years, Mr Van Damme emphasised collective awareness of emerging digital risks, Ms Bouligaraki highlighted partnerships among Member States, and Ms Uudeberg reiterated that shared understanding and determination to find solutions were essential to achieving true digital sovereignty in Europe.

Digital sovereignty can be defined through resilience, reduced dependence on proprietary software, supply chain diversity, avoidance of external strategic control, and interoperability.

PANEL I

Towards Technological Sovereignty: Critical Systems

Moderator:
TAAVI PEHME
Head of the Digital Solutions Operations Department, eu-LISA

This panel explored the role of technologies such as AI, biometric recognition, as well as topics like open-source software and standardisation, in mitigating risks and in strengthening technological independence and transparency. It also looked at how achieving technological sovereignty in critical technological infrastructures such as cloud computing, IT equipment, or communication networks can support the strategic autonomy of the EU.

Panellists:

OTT VELSBERG
Chief Data Officer, Estonian Ministry of Justice and Digital Affairs

LINNAR VIIK
Member of the Board, Mobi Solutions

SAMUEL MARCHAL
Research Team Leader, VTT

RUI MARTINS LOURENÇO
Senior Solution Manager, EUIPO

Taavi Pehme, head of the Digital Solutions department at eu-LISA, acted as moderator and framed the discussion around the technical direction required for reaching digital sovereignty.

Asked about technical gaps that remain to be closed, Ott Velsberg explained that in the past five years Estonia had prioritised cloud adoption, with 62% of Estonian companies using cloud services—well above the EU average. However, Estonia had one of the lowest levels of national AI computing capacity per capita in Europe, fifteen times less than Finland. To address this, the Estonian government had launched the "AI Gigafactory" initiative, which received major funding in July 2024 for GPU infrastructure to serve the public sector. Mr Velsberg emphasised the importance of risk assessment and mitigation for proprietary tools such as large language models, noting that most leading models were non-European. Estonia aimed to develop both cloud-based and on-premise AI capabilities, collaborating with global providers like Google while promoting local resilience.

On cyber-security risks, Samuel Marchal warned that dependence on foreign software and hardware created severe supply chain risks. He stressed that European organisations often relied on external AI components, including U.S. or Chinese-developed foundational models and computing platforms like AWS or Azure. He argued that current benchmarks evaluated AI performance but not integrity, security, or bias, and that Europe lacked mechanisms to assess hidden vulnerabilities or backdoors in such systems.

On European priorities and troubles, Linnar Viik stated that Europe's biggest problem was the widening digital maturity gap among Member States. While some regions had strong digital hubs, others lagged far behind, making EU-wide technical advancement difficult. He argued that Europe needed to first equalise its digital foundations before progressing toward complex sovereign systems, stating that: *"we cannot speak about the next level of European technical advanced systems until we are capable of fixing the basics of digital maturity and architecture at the member-state level."*

Mr Velsberg added that in Estonia, sectors such as finance had over 60% AI adoption, whereas industries like mining had almost none, reflecting deep disparities. Data-intensive companies had grown by 16.2% over two years, with AI-related jobs comprising up to 40% of ICT employment, but digitisation remained uneven.

On short-term changes for the EUIPO, Rui Martins Lourenço described the organisation's cloud strategy, which began in 2019 and was now shifting towards a sovereign multi-cloud model. Out of 120 systems, the agency planned

to return the most critical applications—such as those handling trademark filings—to its own data centres to ensure service continuity. He recalled how a recent power outage in Portugal and Spain had reinforced the need for resilient infrastructure. The new strategic plan to 2030 would prioritise AI integration for trademark and design examination, emphasising sovereignty and data security. EUIPO used models like Mistral, which, though less powerful than U.S. systems, met its specific needs while enhancing autonomy.

On balancing cost and quality, Mr. Velsberg supported testing multiple AI models to balance accuracy, cost, and compliance, and called for investment in European providers. He cautioned that widespread individual use of AI tools—45% of Estonian executives and 37% of public-sector employees—had outpaced organisational readiness, creating risks of unregulated data sharing.

On priorities in the research field, Mr Marchal noted that practitioners struggled to apply new EU regulations because they lacked technical standards. He emphasised that while the EU was quick to legislate, it lagged institutions like the U.S. NIST or MITRE in defining practical frameworks for AI security.

Mr Velsberg added that EU standardisation processes involved thousands of stakeholders and often finalised standards only weeks before compliance deadlines, leaving little time for adaptation.

On EU's digital future to 2030, Linnar Viik predicted a "bumpy road" due to political and technological misalignment. He warned that most Europeans might soon use non-sovereign but interdependent AI systems because companies would prioritise efficiency and competitiveness over political ideals. He expected a surge in AI adoption by 2026 as businesses sought productivity gains from application-level tools, even if they depended on non-European technology.

On data security, Mr Marchal advocated for a "zero trust" approach, continuously testing and monitoring all components, while Mr Viik noted that even rigorous testing could not fully secure systems built on untrusted infrastructure such as Huawei networks.

When audience voting showed digital skills and talent development as the top priorities, Rui Martins Lourenço agreed, highlighting EUIPO's "AI driving licence" programme that made AI literacy mandatory for all staff. Samuel Marchal added that Europe trained highly skilled AI researchers but failed to retain them due to lower salaries and fewer cutting-edge opportunities compared to the U.S. Mr Velsberg reported that Estonia aimed for 80% of its citizens to have basic data and AI literacy by 2030, launching national education initiatives from primary school onward.

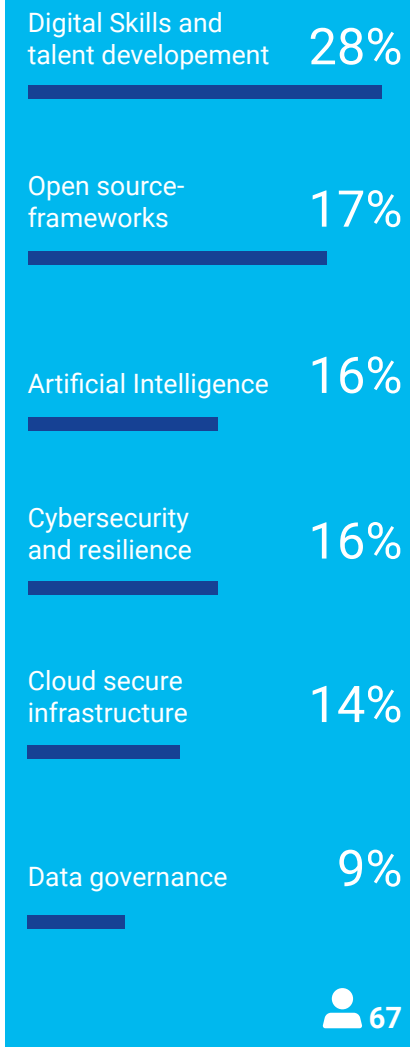
Linnar Viik then connected cybersecurity and digital skills, arguing that both required continuous effort rather than one-off campaigns. He criticised proposals to ban digital devices in schools and praised Estonia's new "AI Leap" initiative integrating AI education into all curricula. At the European level, he advocated for practical interoperability, citing Estonia–Finland cooperation as a model.

In response to a question on investment in adult and law enforcement training, Mr Velsberg explained that Estonia retrained about 10% of central government employees annually, running targeted programmes for data stewards, analysts, and AI champions to spread expertise across ministries.

In closing, the need for true "portability by design," allowing data and systems to move freely between providers to avoid vendor lock-in, especially in times of geopolitical instability, was emphasised. The moderator concluded that collaboration, targeted investment, and collective commitment were essential for achieving resilient and sovereign European digital infrastructure.

WHAT DOES THE AUDIENCE THINK?

Which key area(s) should the EU prioritize for investment to reduce dependency in critical systems?



The foreseen surge in AI adoption is not reaching all sectors or EU Member States equally and work needs to be done on fixing the basics of digital maturity.

PANEL II

Rule of Law and Autonomy: Strategic Technological Choices in the EU Legal Framework

Moderator:
ALEXANDRU LASCU
Head of the Procurement and Contract Management Unit, eu-LISA

This panel explored how different recent legal initiatives and instruments, such as the AI Act, Protect EU, Data Act, NIS2, GDPR, law enforcement directives, etc reinforce sovereignty. Discussions delved into ways governance and procurement choices can help prioritise European providers and technology ecosystems and how the protection of the EU's core values through the rule of law represents a reassurance in the pursuit of strategic autonomy.

Panellists:

TOBIAS BROSER
Head of the Information Management and Innovation Unit, Europol

LENA DÜPONT
Member of the European Parliament

UKU SÄREKANNO
Deputy Executive Director, Frontex

FANNY COUDERT
Deputy Head of the Supervision and Enforcement Unit, European Data Protection Supervisor (EDPS)

The moderator, Alexandru Lascu opened the debate by emphasising that the EU relied on its core values, translated into legal instruments, to shape its technological future. He noted that over recent years several frameworks directly impacting technological sovereignty—including the AI Act, Data Act, GDPR, and law enforcement directives—had been adopted and that the challenge today was ensuring these instruments effectively reduced dependency, strengthened Europe's tech ecosystem, and provided secure, rights-based solutions.

Asked which EU legislative act seems the most important for a future technological framework, Tobias Broser, Head of Unit for Information

Management at Europol, highlighted the Information Exchange Directive, which entered into force in December 2024, as a transformative yet lesser-known piece of legislation. He explained that it established common standards, roles, and procedures for information sharing across EU Member States, greatly improving trust and interoperability between national authorities.

Lena Düpont, Member of the European Parliament and member of the LIBE Committee, agreed and noted that she had served as rapporteur for the directive. She acknowledged that while the EU had made strong progress with regulations and directives, it often struggled to stay technologically up to date. She used the AI Act as an example of how legislation could "freeze" a technological moment that had already evolved by the time the law took effect. She stressed that the key challenge was *"to see how these laws work in practice and where they need to be repaired."*

Uku Särekanno, Deputy Executive Director at Frontex, added that European leaders were increasingly discussing deregulation due to the growing complexity of overlapping legal acts. He pointed to the upcoming launch of the Entry/Exit System on 12 October 2025, the Frontex Regulation, and the EU agencies' data protection framework as areas of intense operational focus. Mr. Särekanno stated that if one examined the different legislative acts, it was clear that the EU was still in a "piloting phase" in balancing internal security with privacy rights.

Fanny Coudert, Deputy Head of the Supervision and Enforcement Unit at the European Data Protection Supervisor (EDPS), emphasised that all EU legislative initiatives were expressions of European values. She outlined that the real challenge lay in operationalising these values—translating them into practical implementation. She also noted that

the EU's regulatory frameworks should not only protect citizens' data within its territory but also govern what digital and physical technologies were imported, *"because we have to regulate what arrives in the Union to ensure it matches our values."*

When asked about the LIBE Committee's role in safeguarding EU core values, Lena Düpont explained that its mandate covered civil liberties, justice, and home affairs. She emphasised the need to balance fundamental rights and privacy with citizen security and called for faster decision-making, as lengthy legislative processes risked obsolescence in a rapidly changing technological environment.

Tobias Broser added that the EU had accumulated so many overlapping legal frameworks that frontline officers often struggled to understand which rules applied. He proposed a "cleanup exercise" to simplify and consolidate *"what exactly is in the realm of the current applicable legal frameworks."*

Addressing Europe's global role, Uku Särekanno stated that instruments like the GDPR had established the EU as a global standard setter, as companies worldwide had to align with EU rules to access its internal market. However, he noted that this influence was weaker in the security domain, where international partners such as the United States were less receptive to EU standards.

The Frontex Deputy Executive Director outlined that the EU should focus on optimising existing tools—like data-sharing between Europol and Frontex—rather than introducing new waves of legislation.

Regarding embedding data protection rules in system governance, Fanny Coudert explained that embedding data protection by design in system development was both a methodological and strategic tool. It allowed the EU to operationalise its values, control data flows, ensure accountability, and enhance strategic autonomy by ensuring that technological systems were built around privacy and transparency from the start.

Turning to cloud technologies, Tobias Broser said Europol was cautiously moving toward cloud adoption due to the scale of modern data analysis, citing the 2022 Sky ECC investigation, which involved over 500 million datasets. He stressed that trust and certification were essential for any transition and that cloud systems should ideally be EU-operated, EU-certified, and hosted on European soil. He mentioned worth exploring the idea of a European agency-run cloud, possibly managed by eu-LISA, to strengthen autonomy and data security.

On aiding EU providers and technology ecosystems, Lena Düpont supported the need for innovation and resilience, arguing that before adopting new regulations, the EU should focus on fixing inconsistencies in existing ones. She called for better coordination between agencies, more efficient resource use, and prioritisation of critical infrastructure, redundancy, and cybersecurity.

When audience polling identified defence and security as the top priorities for strengthening EU strategic autonomy, Ms. Düpont remarked that this reflected the geopolitical realities of the time and urged faster action.

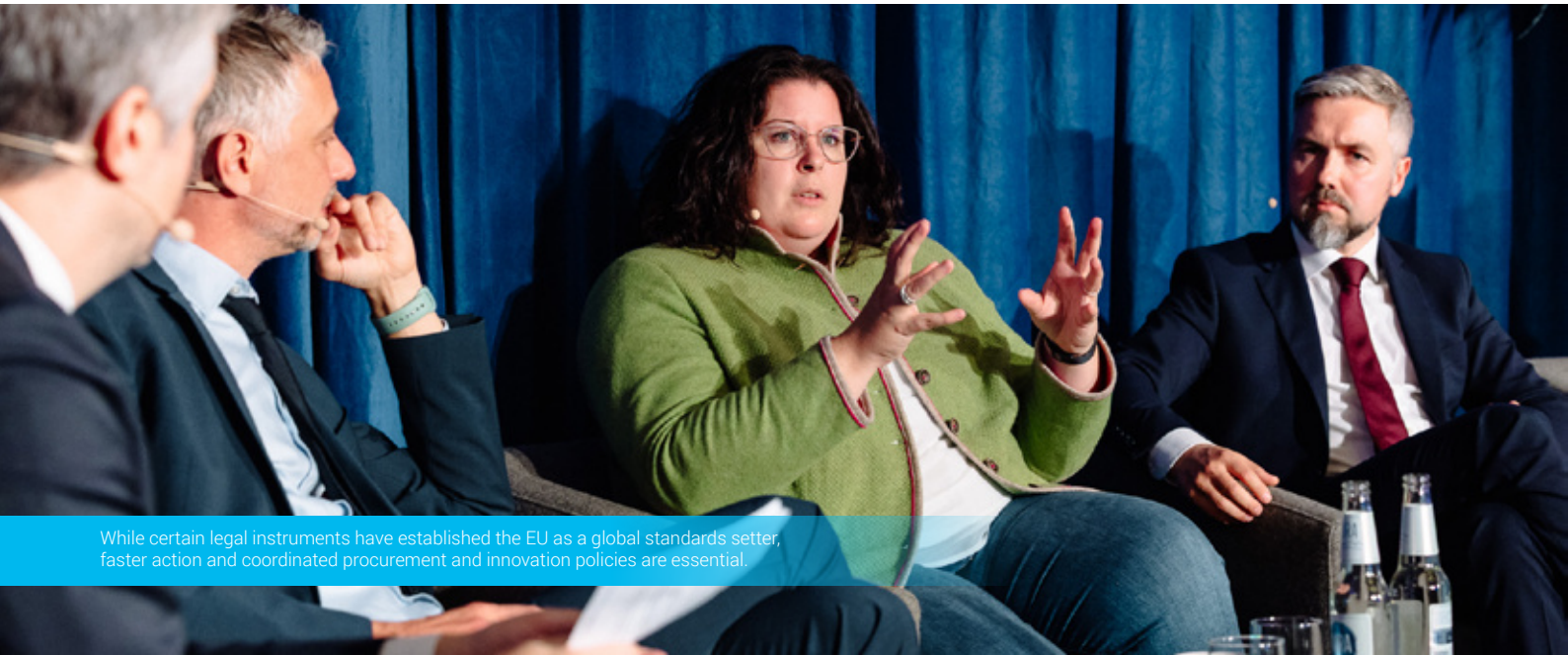
Discussing the Europol Innovation Lab, Tobias Broser explained that it focused on practical, hands-on innovation rather than fundamental research. The lab aimed to close operational capability gaps across Member States by coordinating innovation efforts, converting implicit expertise into shared knowledge, and fostering collaboration through the EU Innovation Coordination Board (EUCB). He also mentioned Article 33a of the Europol Regulation, which allowed the use of operational data for R&D purposes, enabling AI tools to be trained on real data through a secure sandbox environment.

On public procurement, Uku Särekanno stated that the EU's most effective leverage over global tech giants lay in the size of its internal market, not in restrictive procurement. He argued that Europe should use market access as a tool to shape corporate behaviour rather than limit competition in tenders, though he supported excluding suppliers that violated fundamental rights, citing the Huawei example.

Fanny Coudert added that procurement processes could serve as a mechanism to embed minimum data protection and ethical standards in all purchased technologies. Lena Düpont concluded that procurement reform, linked to the White Paper for European Defence, EU Preparedness Union Strategy, and ProtectEU, could help build a more integrated European technological ecosystem. She emphasised that nurturing European providers through coordinated procurement and innovation policies was essential to strengthening the EU's technological sovereignty.

WHAT DOES THE AUDIENCE THINK?

What are the major area(s) in which the EU should adapt legislation to enhance its strategic autonomy?



While certain legal instruments have established the EU as a global standards setter, faster action and coordinated procurement and innovation policies are essential.

PANEL III

Tech Skills for Strategic Autonomy: Developing and Retaining Talent

Moderator:
KRISTI TÄHT
Head of the Human Resources Unit, eu-LISA

This panel explored how to build the technical skills needed to operate and secure digital systems, and how to align talent development with long-term strategic needs. The panel discussed initiatives and ideas that support the development of technological expertise and competences, as well as ways of retaining and using this expertise in the EU market. Additionally, the reskilling dimension and the importance of multidisciplinary training were addressed.

Panellists:

ARNAUD CASTAIGNET
Vice-President, Skeleton Technologies

LAURA HALENIUS
Senior Lead, Sitra

ARNE ANSPER
Chief Technology Officer, Cybernetica

MAILIS PUKONEN
Head of the Strategic Planning and Directorate Unit, CEPOL

The moderator, Kristi Täht opened the pane by noticing that digital skills had been a recurring theme throughout the day's discussions and invited the panellists to explore their importance for Europe's strategic autonomy.

On EU strategic autonomy, Laura Halenius began by explaining that the European Union had identified a range of critical technologies—such as quantum computing, artificial intelligence, semiconductors, space technologies, and cybersecurity—as essential for its future autonomy. Ms Halenius highlighted that the EU needed to attract top global talent, strengthen research, and develop training programmes not only for specialists but for all citizens through large-scale upskilling, because "these technologies are changing our society incredibly quickly." Ms Halenius shared an example from Finland, where Sitra had funded cybersecurity-focused military training for young conscripts, resulting in successful start-ups and ongoing investment. She suggested that such initiatives should be expanded across Europe.

When asked about skills gaps in industry, Arnaud Castaignet described a significant shortage across the European high-tech and energy storage sectors. Using the battery industry as an example, he said Europe had focused on building manufacturing capacity but neglected the broader value chain, remaining dependent on machinery and expertise from Asia. He noted that similar challenges existed in AI and data centres, where Europe lacked capabilities such as GPU design. Mr Castaignet argued that Europe repeatedly celebrated industrial milestones without addressing the deeper technical competencies required for strategic autonomy.

Mailis Pukonen added that CEPOL's European Strategic Training Needs Assessment (ESTNA), which evaluates law enforcement training gaps, had consistently identified digital skills as the top deficiency. She said that while the EU recognised the problem, it lacked systematic monitoring or sufficient investment to address it. She urged coordinated national and EU-level efforts to close these gaps through sustained implementation and collaboration.

On how technological advances and AI had changed the profile of cybersecurity professionals, Arne Ansper warned that reliance on global platforms had eroded Europe's ability to maintain mission-critical systems autonomously. The foundational technical expertise—hardware, networking, and data centre management—was disappearing, as fewer professionals were trained in these lower-level technologies. Mr Ansper cautioned that excessive cloud adoption could compromise autonomy and that efficiency gains should not come at the expense of sovereign capability.

When asked about challenges in attracting skilled professionals to public institutions, Ms Pukonen noted *"the problem lies not solely in attraction – because the truth is there are not enough people to attract. One company's successful recruiting win is another's loss."* She identified several barriers,

including slow and rigid recruitment procedures that could take up to eight months, non-competitive salaries, and complex security clearance requirements. Potential solutions were outlined, such as creating faster recruitment mechanisms, offering fellowships and mobility programmes with academia and industry, and emphasising the EU's mission-driven purpose to compensate for lower pay. Ms Pukonen added that mobility and location were also challenges, as many EU agencies were based in less attractive cities and constrained by language and administrative rules.

On sustainable upskilling, Laura Halenius proposed practical solutions such as introducing EU-wide security clearances to allow experts to move across borders more efficiently, noting that the current system, where each clearance process could take up to eighteen months per country, was unnecessarily restrictive.

On balancing corporate interests and the EU aim for digital sovereignty, Arnaud Castaignet, responding to the poll results showing upskilling and reskilling as participants' top priority, stated that he felt this to indeed be the key priority. He described how modern manufacturing increasingly relied on digital twins and automation, requiring engineers to master both hardware and software skills. *"In order to digitally automate you need people who are able to understand both digital*

tools and hardware." He warned that Europe lagged behind Japan and South Korea in factory automation and robotics and that regions needed to attract new talent while retraining existing workforces to adapt to high-tech industries.

On training methods, Mailis Pukonen stressed that multidisciplinary education was essential. She said CEPOL's courses now integrated horizontal issues such as ethics, fundamental rights, and regulatory awareness to help law enforcement officers operate in a complex digital environment. Training was shifting from classroom-based to blended learning, allowing continuous follow-up and impact assessment. She underlined that officers needed to understand both legal frameworks and AI ethics to maintain public trust.

Laura Halenius then expanded on the role of partnerships between academia and industry. She noted that only 200 of 1,000 ICT graduates in Finland were sufficiently prepared for advanced AI work. She argued that the EU needed top research centres of excellence in critical technologies, citing Finland's newly established Ellis Institute as a successful model supported by public-private cooperation between Sitra, Silo AI, and AMD. She also highlighted the LUMI supercomputer, one of the world's most energy-efficient systems, as an example of infrastructure that attracted global talent and enabled companies such as Silo AI to grow into European unicorns.

On long-term threats to Europe's technological capabilities, Arne Ansper warned that declining mathematics education posed a significant problem, observing that mathematics teaching had become overly simplified, depriving students of abstract thinking skills essential for cryptography, AI, and system design. He said Estonia was already facing a shortage of cryptographers and warned that foundational knowledge, not just technical training, was crucial for sustaining innovation. Arnaud Castaignet agreed that critical thinking and abstraction education were increasingly rare. He noted that in his sector, mechanical and chemical engineering skills had become harder to find. He emphasised the need for versatile professionals capable of bridging disciplines, understanding both digital tools and physical systems, and collaborating across teams rather than working in silos.

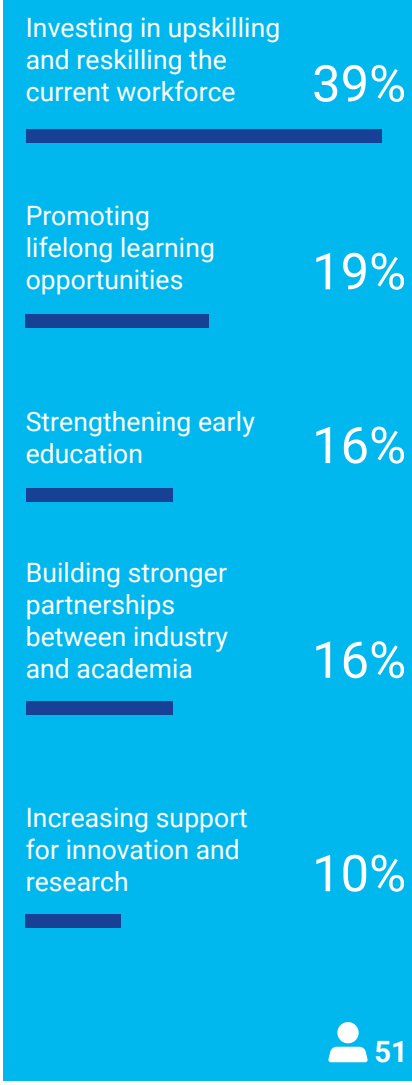
In closing remarks, Mailis Pukonen stressed that Europe not only needed to attract but also to multiply existing expertise through knowledge management, train-the-trainer schemes, and EU-wide centres of excellence to share best practices and deliver joint training programmes with industry.

Laura Halenius concluded that Europe must create mission-driven talent pathways starting from school, citing Finland's long-term investment in quantum research since the 1970s as an example of how consistent strategy produced world-class expertise.

Arne Ansper added the priority should be improving general education systems to sustain future innovation, while Arnaud Castaignet called for a more practical link between academia and industry, enabling Europe to convert its research excellence into scalable technologies, products, and businesses. He argued that Europe's attractiveness should be directed toward strengthening skills and industries critical for achieving strategic autonomy.

WHAT DOES THE AUDIENCE THINK?

What should be the top priority(ies) for reducing the digital, science, and technology skills gap?



Investing in upskilling and reskilling the current workforce, as well as improving general education systems to sustain future innovation should be seen as priority.

PRESENTATION

Border Management & Security: Through the Lens of the JRC

Presentation by

MATTHIAS OEL

Director, Joint Research Centre (JRC), European Commission

Matthias Oel, Director, Joint Research Centre (JRC), European Commission, began by noting that the discussion on strategic autonomy was particularly relevant in light of the dramatic geopolitical changes facing Europe, highlighting ***"that the current geopolitical situation and the decrease in multilateral cooperation forces the EU to increase its autonomy"***.

Mr Oel introduced the Joint Research Centre (JRC) and its new Border Security Laboratory, launched on 10 April 2025 to serve as a collaborative research hub for EU agencies and Member States. The laboratory was developing a dedicated research infrastructure at the JRC's Geel site in Belgium and would focus on external border management, digitalisation of travel processes, and facilitation of secure paperless border crossings. The forthcoming Security Research and Innovation Compass, a JRC initiative mentioned in the EU's Internal Security Strategy and planned to be officially launched in the first quarter of 2026 was also presented. The Security Compass is aimed at making the JRC a central hub for European security, Mr Oel adding that *"everything is evolving at lightspeed and so we must pool our resources"* and research by bringing together operational agencies, scientists, and policymakers.

Mr Oel concluded by stressing that only close collaboration among Commission services, EU agencies, and Member States could ensure secure borders and trusted technologies for the future.

PRESENTATION

eu-LISA's Contribution to EU and Member States Sovereignty

Presentation by

THEOFANIS SYRIGOS

Head of the Programme and Solutions Management Unit, eu-LISA

Mr Theofanis Syrigos's presentation outlined eu-LISA's contribution to European and Member States sovereignty, echoing themes such as balancing independence with practical solutions, and the call to action, which accurately reflects eu-LISA's approach: achieving independence through concrete, efficient action. *"We know what to do, so let's just do it."*

The launch of the Entry/Exit System on 12 October represents a historic moment and the first operational step toward building the technological and decision-making foundations of European sovereignty. The scale of the system and its role in supporting border, visa, immigration, law enforcement authorities, as well as the carriers, were emphasised. By automating checks and supporting faster decision-making, EES will enhance security and maintain Europe's openness, making Europe's borders more efficient rather than restrictive, which represents a "triggering event" for building the practical conditions of European sovereignty.

Part of a larger ecosystem of interconnected IT systems being developed by eu-LISA, the interoperability architecture will transform raw data into actionable information for decision-makers, marking a major step toward EU-level IT sovereignty. Moreover, by centralising complex and costly technical functions, the agency reduced duplication, lowered costs, and allowed national governments to allocate resources to other priorities, while ensuring that sovereignty in decision-making remains independent at the national level.

In conclusion, eu-LISA's mission was summarised as *"connecting the dots to enhance an independent and sovereign decision-making capacity of EU Member States, in full respect of their independence."*

WRAP-UP & CONCLUSIONS

Conclusions by

LORENZO RINALDI

Head of the Business and Stakeholder Relations Unit, eu-LISA

Lorenzo Rinaldi, Head of the Business and Stakeholder Relations Unit at eu-LISA, concluded the 2025 eu-LISA High-Level Conference by thanking all distinguished speakers, colleagues, and guests for their engagement, openness, and forward-looking spirit throughout the event.

Mr Rinaldi recalled that the day had been filled with substantive discussions on European sovereignty and technological independence, with the emphasis that strategic autonomy was not merely about technology but also about values, asserting that Europe's sovereignty should preserve its ethical principles while fostering creativity and independence in decision-making.

Looking ahead, Mr Rinaldi highlighted the upcoming milestone on 12 October—the launch of the Entry/Exit System—which he described as one of the most significant achievements in eu-LISA's history.

He assured participants that eu-LISA would remain at the centre of the ongoing effort as both a user and steward of critical technologies and as a trusted partner of EU institutions and Member States. Strategic autonomy, he stressed, was a shared responsibility that could not be achieved in isolation. Mr Rinaldi concluded the conference by highlighting that strategic autonomy *"is not a static achievement. It is an ongoing collective effort which requires coordination, investment, resilience, imagination, and courage; and rest assured that eu-LISA will remain as both a user and steward of this collective effort."*

ISBN: 978-92-95237-06-3
DOI:10.2857/3476749
Catalogue Number: EL-01-25-010-EN-N