ECSO Feedback to the EU Startup and Scaleup Strategy

SME2Market Workstream

Cybersecurity Market Development Working Group

Ver. 1.0 14/03/2025

Introduction

Context and Purpose

The European Commission (henceforth EC) opened a call for evidence for the **EU Startup and Scaleup Strategy** (or the Strategy), in its "Have your Say" Portal, on the 17th of February 2025. The deadline for providing evidence to the Strategy is set to the 17th of March. The EU Startup and Scaleup Strategy is "a strategy to improve conditions for innovative startups and scaleups, enabling faster and simpler growth within the Single Market" (EC, 2025).

The European Cyber Security Organisation (ECSO in short) is a public-private association at the European level in the cybersecurity ecosystem, which started in 2016 under a contractual Public-Private Partnership with the European Commission until 2020. ECSO has a member base of around 350 members from the public and private sectors, namely public administrations, universities, regional authorities, large companies, SMEs, investors, associations, clusters, research organizations (RTOs), among others. It aims to increase European Digital Resilience and Strategic Autonomy in the cybersecurity ecosystem, supporting European innovation and growth across Europe.

ECSO has a strong legacy of supporting European startups and scaleups in cybersecurity, in driving investment in the sector via its European Invest4Cyber community and fostering the uptake of cybersecurity solutions via its European CISO Community and the launch of the first European digital marketplace, the Cyberhive Europe. Furthermore, as an industry representative, with over 140 SMEs and 40 large providers of cybersecurity services and its diverse private and public sector member base, ECSO aims to relay the views of the European cybersecurity community to the EU Startup and Scaleup Strategy.

ECSO will achieve this by providing evidence in the current open call for evidence, but also by continuing its engagement with the European Commission and opening a dialogue on the Strategy, and engaging in the consultation process, ensuring its member's positions are reflected in the Strategy.

Executive Summary

Key findings

ECSO agrees with the hurdles identified in the document of the call for evidence and further provides details on its member's insights into their impact in the cybersecurity community:

- **Access to finance:** There is a significant funding gap in the European cybersecurity market, with venture capitalists being risk-averse and unable to provide the large investments needed for scaleups.
- **Regulatory and bureaucratic burdens:** Cybersecurity startups face complex and diverse regulatory frameworks across Europe, requiring them to navigate different

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

national standards and certifications, which increases costs and slows down growth and innovation.

- **Access to market:** European cybersecurity solutions are often overlooked in favour of American providers, and there is a lack of strategic procurement by European institutions to support local solutions.
- **Access to talent:** The cybersecurity sector in Europe suffers from a workforce and skills gap, gender disparity, and brain drain, making it difficult to find and retain qualified professionals.
- **Access to research and technology infrastructure:** There is unequal availability of research and technology infrastructure across European member states, leading to compartmentalized knowledge and unequal development in the cybersecurity sector.

ECSO recommendations

Based on these hurdles, through a consultation effort with its members and its own initiatives and advocacy activities since 2016, ECSO has put forward several recommendations for the Strategy:

- **Increase market impact of EU funding:** Increase EU funding availability for startups and scaleups, focusing on projects that bring innovative solutions to market, and ensure consortia include diverse participants to facilitate market application.
- **Harmonise and recognise standards:** Harmonize European standards, and adopt mutual recognition agreements for national standards and certifications to enable startups and scaleups to serve different customers and leverage public procurement processes.
- **Invest in networks of incubators and accelerators:** Establish a European network of sector-specific incubators and accelerators to support startups and scaleups with mentorship and expert advice, helping them grow in diverse markets.
- **Celebrate European solutions:** Develop communication campaigns with partners to highlight success stories of European cybersecurity players, promoting their capabilities and contributions to the digital ecosystem.
- **Drive competitiveness:** Encourage tax incentives for EU-based startups, support market consolidation to create European champions, and facilitate the growth of the European VC ecosystem through competitive providers.
- **Leverage procurement:** Use strategic purchasing power to promote European industry by mandating European participation in procurement processes and prioritizing European consortia and SMEs.
- **Attract and develop talent:** Offer incentives to attract top foreign talent, emphasize the link between capital access and talent retention, develop industry-collaborative professional courses, and motivate European-trained talent to stay in Europe post-graduation.
- **Promote European solutions in international markets:** Adjust trade agreements to support European cybersecurity companies' access to non-EU

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

markets, prioritize global digital infrastructure investments with European cybersecurity solutions, and establish EU trade delegations to major conferences and events.

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

ECSO's Feedback to the EU Startup and Scaleup Strategy

ECSO supports the findings in the political context and problem definition of the document of the call for evidence for the Strategy. The hurdles identified in this document, namely the limited access to finance, the regulatory and bureaucratic burdens and fragmentation, the difficult access to EU markets, the constraints in access to talent, and the limited access to research and technology infrastructure, are current obstacles faced by startups and scaleups in the cybersecurity sector.

These hurdles prevent effective innovation and growth of European native cybersecurity solutions, and cause a big drain on European champions, as they move to other more competitive markets, which do provide the needed conditions for these companies to achieve their full growth potential.

Key findings from the ECSO community

Through a dedicated consultation action to its members, as well as its previous advocacy actions, ECSO has derived some key findings in the cybersecurity sector that are relevant for the Strategy. As explained above, these findings agree with the problem statement of the Strategy. The goal of this section is to provide further insights from the cybersecurity sector into the identified hurdles.

To facilitate the reading of these findings, they will be mapped to these hurdles.

Access to finance:

- Similar to other sectors, there is a funding gap in the cybersecurity market, demonstrated through different studies (EIB, 2022; ECSO, 2024), of around 1.75 billion euros in 2022. The current funding gap as of 2025 likely reaches higher values, considering the growth of the market and the decrease in private investment in cybersecurity since 2022 from 2.44 to 1.25 billion euros (Tikehau Capital, 2024; ECSO, 2024).
- The cybersecurity venture capital ecosystem in Europe cannot accommodate the largest tickets required to fuel the growth of scaleups.
- European venture capital has a shorter target investment duration of 5-7 years, which hampers their impact and capacity to support European cybersecurity startups.
- The European cybersecurity market is not an active sector for exits. The small presence of development capital, large cybersecurity and digital players and integrators present or interested in this sector delays the exits of the existing investments, which in turn slows the growth of the VC ecosystem. Most of the exits are realised by American companies and investors (ECSO, 2024).
- There is a lack of public-private partnerships, except around cybersecurity and defence. And these often escape the dual-use technologies, or focus on pure-defence, curtailing the capital available for the civil sector of cybersecurity, and

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

failing to explore the vast potential for public-private investment in the cybersecurity sector, leveraging on the defence needs and current geopolitical trends, to drive the growth and innovation of this crucial sector.

- Compared to the American VC ecosystem, the European cybersecurity VC players are considerably more risk-averse, and do not risk in providing the needed capital to more risky and innovative startups, which results in a lack of European-native champions from inception, as the startups also adapt their innovation to a longer investment cycle, effectively slowing the innovation clock in Europe, compared to other geographies.

Regulatory and bureaucratic burdens

- Every time a scaleup seeks to expand across Europe, they need to open a new branch, where local/national teams and expertise needs to be involved to address the different regulatory frameworks, different bureaucratic realities around taxes and employment, among others. This implies that the cybersecurity startups and scaleups operating across multiple members states must replicate structures across different national realities to address their specific frameworks, preventing them to benefit from economies of scale at the European level.
- Differing national standards and certifications in cybersecurity around Europe create unnecessary financial burdens for scaleups, who need to obtain these national certifications to be considered legitimate providers in those respective countries. As many European startups and scaleups lack the funding to obtain these standards, as they often imply costly and time-consuming processes, these tend to favour larger providers, normally from non-European origins, who have the resources to obtain these standards across Europe.
- Similarly, regarding investment processes and regulatory frameworks, these are also diverse across member states, further increasing costs and reducing the speed of cybersecurity investments across Europe. As cybersecurity VCs are especially operating at the European level due to small national markets, this is a crucial barrier to their ease to invest.
- Startups lack the resources and expertise to focus on the diverse processes requested from them, such as taxing declarations, accounting, personnel management, standards, compliance, and more. Furthermore, this effectively diverts their time and resources away from driving the innovation of their solution, securing the required funding, and obtaining their first customers.

Access to market:

- There has been a preference in the consumer's choice of cybersecurity solutions, in favour of American providers instead of European ones. Often, large end-users of cybersecurity solutions would prefer the integrated and safer American solutions versus the European one. In addition, the current geopolitical trends, the political and economic instability in the United States, the developing trade war, and the boycotting of the International Criminal Court, will impact European Chief Information Security Officers (CISOs) decision-making and procurement

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

strategies, and likely push them to increasingly prioritise European cybersecurity solutions.

- Europe retains innovative capacity and capability in certain key areas and technologies, despite the dominance of non-European players. There is a preference for non-European providers, and a lack of awareness on European excellence in many sectors, as competitive and innovative European solutions are often overlooked.
- European and national institutions do not leverage their purchasing power sufficiently to support European solutions. There is a lack of strategic procurement to drive the uptake of national and European cybersecurity solutions. Furthermore, the reliance on non-European solutions in these processes also undermines European growth and Strategic Autonomy.

Access to talent:

- With a telling workforce and skills gap in the cybersecurity sector, the strain on access to talent is likely to continue, as Europe struggles to train and educate enough cybersecurity professionals to meet the needs of the industry (ISC2, 2024). The current gap is estimated at 392,320 professionals in Europe (Idem).
- A gender gap is evident in the cybersecurity workforce in Europe, where, on average, only around 22%-24% of professionals in security teams are women (ISC2, 2025). The lack of female professionals in the sector points to systemic factors that make the sector less attractive for female professionals, resulting in a reduced pool of potential workers to address the workforce and skills gap.
- The different employment and tax regulatory frameworks across Europe affect startups and scaleups in the cybersecurity sector, where a distributed workforce working remotely is more common. This further hampers the growth capacity of these innovative companies, as they must contend with different employment considerations for their teams, dedicating time, and resources, to these legal requirements.
- European talent is drawn to non-European education systems and high-paying job opportunities abroad. This brain drain weakens Europe's ability to innovate and compete globally. In addition to retaining European talents, Europe is not able to attract the best professionals from other countries.

Access to research and technology infrastructure:

- In the maturing cybersecurity sector, there are differences between member states and their respective markets in the availability of research and technology infrastructure. The knowledge and expertise in Europe are further compartmentalised across different countries, with specific and specialised markets and knowledge in the member-states. These differences often create unequal developments across the member-states that have increased capacity and lead in innovation, when compared to smaller countries that do not have the same capacity to drive research and innovation activities. This drives unequal outcomes in research activities throughout the European Union.

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

- As startups and scaleups often lack expertise in diverse domain areas needed to thrive in Europe (not the least of which to navigate complex regulatory frameworks), the needed personnel and skills to effectively navigate the diverse cultural and linguistic realities in Europe, and the networks and market-specific knowledge to integrate different national markets, they are often constrained and require support and advice from experts and entrepreneurs to maximise their growth.
- The incubators and accelerators in the cybersecurity sector are scattered and often staffed by young workers that lack the entrepreneurial and innovation experience and networks required to properly support European startups and scaleups to grow.

Recommendations for the EU Startup and Scaleup Strategy

The recommendations that are construed in this document result from the dedicated consultation undertaken by ECSO with its members, through an in-depth discussion with its SME2Market Work Stream chairs, but also through a dedicated survey run by the organisation's members. Furthermore, these recommendations are the product of ECSO's own activities since 2016, its interaction with the industry, and the inputs of its members throughout this period across its many initiatives.

The ECSO Secretariat has compiled all these inputs into the recommendations below.

Increase market impact of EU funding

- Increase the availability of funding from European institutions and programs for startups and scaleups with a focus on concrete projects that result in innovative solutions that are introduced to the market, making the application of EU funding more efficient in supporting the growth of European native technology.
- Ensure consortia include not only universities and research organisations, but also startups, scaleups, and larger providers, to facilitate the market application of the project.
- Enable European funding to reach existing scaleups with a proven market acceptance, accelerating the developments of existing capacities and capabilities and the growth of European companies.

Harmonise and recognise standards

- Harmonise different standards and certifications throughout the EU across its different sectors would ensure that startups and scaleups have the capacity to service different customers across the Union and be certified to provide services to the different national governments and leverage public procurement processes to accelerate their growth.
- Similarly, more mutual recognition agreements for national standards should be adopted, to ensure that if startups and scaleups obtain a certification in one member-state, it is recognised by the other states.

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

Invest in networks of incubators and accelerators

- Establish a European network/federator of sector-specific incubators and accelerators, to support startups and scaleups in developing innovative solutions and growing in Europe's diverse markets. These incubators and accelerators should provide startups and scaleups with support from mentors and experts by creating incentive programs to attract experienced entrepreneurs and potential advisors to these accelerators, with developed networks in the sector and country these companies seek to grow to.

Celebrate European solutions

- Develop structured communication campaigns in collaboration with all relevant partners, including, but not limited to, the European Commission, ENISA, and EEAS, to highlight success stories of European cybersecurity players.
- Promote success stories highlighting European capabilities, strengths, and their contribution to developing the robust European digital ecosystem.
- Ensure that the exemplary European cybersecurity solutions are mentioned in relevant institutional engagements with non-European counterparts.

Drive competitiveness

- Encourage Member States to introduce tax incentives for EU-based startups, particularly those with less than 20% non-EU investment.
- Create incentives to support the consolidation of the market and create European champions from integrating innovative scaleups and larger European providers, effectively creating European champions and aggregators, which can compete in the international market. These competitive providers will then be able to acquire innovative startups and scaleups, which in turn facilitates the growth of the European VC ecosystem.

Leverage procurement

Leverage strategic purchasing power to bolster European industry, drive innovation, and promote sustainability by:

- Mandate European participation and promoting a 'Buy European' mindset, setting a baseline target for European participation in procurement processes, with a minimum of 30% of evaluated bids being from European companies in crucial sectors such as cybersecurity.
- Promote European consortia and SMEs, prioritizing European consortia and companies with cross-border structures and SME involvement to foster collaboration and growth within the European ecosystem.

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

Attract and develop talent

- Encourage Member States to offer incentives, including tax benefits and streamlined visa processes, to attract top foreign talent to the EU.
- Underscore, in all communications regarding skills and talent, the critical connection between access to capital and the ability to attract and retain top-tier talent.
- Encourage academia to develop professional courses organised in close collaboration with industry representatives, providing firsthand experience and coaching.
- Offer incentives to motivate European-trained talent to remain in Europe for a specified period post-graduation.

Promote European solutions in international markets

- Adjust trade agreements to support European cybersecurity companies' access to non-EU markets and ensure no tariff are imposed on them.
- Prioritise the development of global digital infrastructure investments, with a specific focus on integrating cybersecurity solutions provided by European entities, as this strategic approach will generate a powerful spill-over effect, fostering robust cybersecurity measures worldwide.
- Establish EU trade delegations to major conferences and events across key sectors, coordinating efforts between member-states and EU institutions to foster the participation of European companies in international conferences and events. Leveraging on the networks and contacts established by EU institutions and member states in non-European countries would provide European startups and scaleups with increased possibilities to engage in accessing non-European markets.

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

Conclusion

Throughout its work, ECSO has strived to represent the voice of the cybersecurity community in front of the European institutions. By submitting this feedback to the call for evidence by the European Commission, it aims to continue to do so, and to provide its members with the possibility to advocate for their points of view and feedback within the framework of ECSO.

Consequently, ECSO will continue to work with its members to bring concrete and actionable feedback to the European Commission form the cybersecurity industry around those initiatives that it believes are of interest to its members, and have an impact within the industry, as is the case with the upcoming EU Startup and Scaleup Strategy.

ECSO and its members are open to participate in any further consultation requested by the European Commission and will be looking forward to engaging with the EC to continue to reflect the cybersecurity community's views on the EU Startup and Scaleup Strategy.

If any further clarifications on the points elaborated in this document are needed, please contact ECSOteam@ecs-org.eu or francisco.andrade@ecs-org.eu.

References

All findings and recommendations are derived from ECSO's activities and its consultation from its members. Any references are meant to support the points that were raised throughout the document.

European Commission. *EU Start-up and Scale-up Strategy*. 2025. Available on: Initiative details.

European Commission. *Special edition: Startup and Scaleup Strategy – Call for evidence*. 2025. Available on: RESEARCH AND INNOVATION - Special edition: Startup and Scaleup Strategy – Call for evidence.

European Cyber Security Organisation. *Home-ECSO*. 2025. Available on: Home - ECSO

European Investment Bank. *European Cybersecurity Investment Platform*. 2022. Available on: European Cybersecurity Investment Platform

European Cyber Security Organisation. *European Cybersecurity Investment Platform - ECSO*. 2025. Available on: European Cybersecurity Investment Platform - ECSO.

ISC2. *2024 ISC2 Cybersecurity Workforce Study*. 2024. Available on: 2024 ISC2 Cybersecurity Workforce Study.

ISC2. *Survey: Women Comprise 22% of the Cybersecurity Workforce*. 2025. Available on: Survey: Women Comprise 22% of the Cybersecurity Workforce

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91

Contributing experts and organisations

The following ECSO members contributed to the draft of the paper:

Jorg Audorsch, ESCRA

Pierre Calais, Neosmos

Regis Cazenave, S2Grupo

Ignacio Sbampato, Excalibur

Francois Lavaste, Tikehau Capital

Ali Marbrouk, SAMA PARTNERS Business Solutions GmbH

Fredrik Standahl, FM CyberSecurity AS

Furthermore, ECSO and its remaining members contributed to the positions in this paper through its multiple activities and advocacy efforts since 2016. All the points brought forward in this document are derived from inputs from the ECSO community.

European Cyber Security Organisation (ECSO) | Avenue des Arts 46, 1000, Brussels (Belgium)
media@ecs-org.eu | ECSO is registered at the EU Transparency registry: 684434822646-91