Joint letter by DIGITALEUROPE and its member associations on the creation of a European Digital Infrastructure Consortium on cybersecurity upskilling

Escalating cyber threats have brought the urgent need for robust cyber preparedness to the top of the EU agenda. The war in Ukraine underscores the need for a comprehensive solution to collective security in particular. Regrettably, the EU finds itself confronted with a projected shortage of **1 million** cybersecurity professionals by 2030,[1] despite promising job opportunities in the field. Compounding this issue, both public and private sector are now required to navigate increasingly complex cybersecurity legal and policy requirements in the EU.

We should call this scenario for what it is: cyber skills development is a labour market failure in the EU. There is a persistent mismatch between the skills demanded by employers and those possessed by the workforce. A robust public-private partnership is now critical to address this challenge. Industry is ready to engage, recognising the urgency and shared responsibility to address the pressing issue.

By 30 May, we encourage you to answer the European Commission's call for Member States to form a European Digital Infrastructure Consortium (EDIC), as proposed in the EU Cyber Security Skills Academy Communication. **This EDIC should focus on setting up and coordinating a network of cybersecurity training campuses across Europe.**

DIGITALEUROPE's network of 41 national digital associations stand willing and ready to provide private sector support. Through our vast membership of 45,000 business members, we are ready to tap into our resources and expertise. We have successfully acquired funding for a pan-European Master's in Cybersecurity in collaboration with academic partners and, together with our national

---

[1] Back-of-the-envelope calculations based on estimates from figures here

digital association, we are creating 7 Cybersecurity Skills Hubs in Europe. This will enhance national skills strategies minimise cybersecurity skills mismatches across Member States and thereby help provide the necessary talent to support future cross-border cyber threat detection platforms at the EU level.

We now need Member State support to make a network of cybersecurity training campuses a reality and close the cybersecurity skills gap.

The network should complement the operations of national ministries, ENISA and the European Cybersecurity Competence Centre. Establishing these campuses would serve as a tangible demonstration of governmental commitment to digital security at a time when global cybercrime costs grew **by 100%** to reach **€5.5 trillion** between 2015 and 2020.[2]

The economic, societal and political benefits of an agile EDIC are too large to ignore. They include:

- More effective EU security: cyber-attacks do not stop at national borders, nor should our efforts to combat them. Localised incidents can quickly spread across the EU without the right incident specialists. SMEs will require unprecedented compliance expertise to implement recent legislation like NIS2, DORA and soon the Critical Resilience Act. **6 in 10** small firms said they may shut down if exposed to serious cybersecurity issues.[3]

- Long-term cost savings: investments to equip the workforce with cyber skills now will reduce the financial impact of any future cyber-attack later. There are also clear budget savings from accessing shared resources and expertise among Member States.

- Global influence in the EU digital discourse: an EDIC for cybersecurity upskilling will forge an even more structured dialogue among private and public sector stakeholders, as well as with NATO and like-minded partners.

Co-signatories:

- AAVIT
- Agoria
- Anitec-Assinform
- GZS
- HGK
- ITL
- IVSZ
- Numeum
- PIIT
- SEPE
- Technology Ireland
- Teknikföretagen
- TIF

---

[2] Council of the EU, Infographic - Top cyber threats in the EU
[3] ENISA, Cybersecurity for SMEs - Challenges and Recommendations, 2021