Europe's cybersecurity potential is not being fully realized due to the existing fragmentation of the cybersecurity landscape and inefficient cooperation and collaboration.

One of the ways to overcome the existing fragmentation is by promoting the already existing and functioning structures, especially at the national level, while actively pursuing the aim of a pan-European community through networking.

The concept of CHECKS ('Community Hubs of Expertise in Cybersecurity Knowledge') as a grassroots bottom-up approach was developed by CyberSec4Europe over the course of the past four years as a way to provide additional involvement channels and complement the bodies and organisations set up by the EU legislation, namely the European Cybersecurity Industrial, Technology and Research Competence Centre, the National Coordination Centres and their network, and the Cybersecurity Competence Community.

These community-level cybersecurity hubs should enable collaboration between industry and academia, bring market security innovations and help build capabilities in the area by shortening the chain between decision-making and existing needs on the ground.

The governance model would benefit from targeted European cybersecurity funding mechanisms in the next decade to build and maintain a pan-European cybersecurity community.
Policy Recommendations

With no active institutional and funding efforts towards ensuring the cohesion of the European cybersecurity community, the rich existing potential of research, skills-building and market applications is in danger of not getting exploited. The new structure based on the European Centre, the NCCs, and the Community pillars needs to include more tangible actions for nurturing and structuring the Community. A cohesive European cybersecurity ecosystem is essential to further develop and enhance the European innovation potential, as well as to ensure European digital sovereignty. Based on the findings of CyberSec4Europe’s work, we offer the following three main policy recommendations:

1) Institutionalise the Cybersecurity Competence Community
   It is key that the National Coordination Centres have a systematic approach to registering communities and hubs. With the Regulation providing no guidelines on how possible members who are not already well networked and informed should learn about the possibility of application and registration, it is important to develop mechanisms to do so. The benefits and added value for possible members to get acknowledged as members of the Community through the application and registration procedure should be made clear.

2) Use CHECKs to organise the Community, in order to address the existing challenges, while providing flexibility
   We offer the concept of a collaborative network of local cybersecurity hubs, ‘Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)’, which are envisioned as environments for community-level research, innovation and capacity building in cybersecurity. This concept answers concrete stakeholder demands and is based on requirements, empirical best practices and stakeholder feedback. The existing diversity in the Member States and their connection to the NCCs and to the Community can be integrated through CHECKs (thus resulting in complementary approaches for addressing the same mission).

3) Dedicate funds to capitalize on the existing community connections and networks
   The H2020 pilot projects (CyberSec4Europe, ECHO, SPARTA and CONCORDIA) and their focus groups, as well as the European Cyber Security Organisation (ECSO) and its working groups, also represent a rich connected community. The majority of relevant stakeholders are involved in the cybersecurity ecosystem through the four pilots and ECSO, forming an ecosystem with different focuses, maturity stages and objectives. Therefore, dedicated funds should be provided, for example, under the Horizon Europe/Digital Europe programmes, to deepen the cooperation and coordination of such stakeholders, alongside dedicated funds to set up CHECKs in all Member States.

References


Contact

This brief was produced by members of the CyberSec4Europe consortium. Contact person: Natalia Kadenko n.i.kadenko@tudelft.nl

cybersec4europe.eu