Cyber Security for Europe

Policy Recommendation

Facilitate cybersecurity collaboration by creating flexible and accessible community engagement mechanisms

Context and Findings

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.

The Problem

The European Union has articulated the ambition to increase its sovereignty and become a global leader in the digital economy, guided by the need both to protect democratic values and to develop the capabilities to be resilient when it comes to cybersecurity threats. The European Commission has accordingly identified four main challenges in the area of cybersecurity that need to be overcome in order to realise this ambition[1]:

- Lack of cooperation between Member States, industry and academia, leading to fragmented efforts in research and development (R&D)
- Insufficient investment in cybersecurity
- Increased demand for skills, know-how and facilities, while access thereto is limited
- Inconsistency of new policies and governance with the existing legal frameworks

Currently, despite the availability of a broad range of talent, cybersecurity cooperation in the EU suffers from the lack of dedicated institutions and structures that would facilitate collaboration, as well as from the under-representation of certain stakeholders who are important for a sustainable approach to R&D, such as privacy and ethics activists.

The Scene

In order to meet these challenges, the European Commission has set up a European Cybersecurity Industrial, Technology and Research Competence Centre, mandated the establishment of National Coordination Centres (NCCs) and their network, and created the notion of the Cybersecurity Competence Community[2].

Several CyberSec4Europe reports assess the best governance practices for the Community. They analysed governance proposals for the various levels of and diverse approaches to cybersecurity governance, tested them against the input required by the relevant stakeholders, and drew conclusions about the desired characteristics of a governance model that would be able to answer the identified challenges.

Through research and practice, CyberSec4Europe explored bottom-up governance approaches and came up with 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. The advantage of such hub structure is a low participation threshold for under-represented actors and the potential to accommodate different types of organisations in order to facilitate coordination.

The Implications

In combating fragmentation in the cybersecurity domain the existence and promotion of "communicating vessels" is of paramount importance. Knowledge should flow where it is needed – i.e., it should be transported between countries and/or sectors to overcome "the cybersecurity divide" of maturity and funding.

This flow of information is important in order to realise the full potential of Europe's vibrant and dynamic cybersecurity community in achieving more engagement and involvement from the grassroots level of cybersecurity in Europe. At the same time, this communication will ensure broader participation from those who may not have the time, the resources or the opportunities to contribute as stakeholders, users, solutions providers, as well as from regulators and public sector agencies.

The Regulation[3] does not provide any organisational structure for the public-private and inter-institutional collaboration between Community members. It is therefore unlikely that the Community will achieve the aim of overcoming the fragmentation of EU cybersecurity stakeholders without additional collaboration mechanisms or dedicated funding.

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

1 See D2.1 Governance Structure v1.0, https://cybersec4europe.eu/wp-content/uploads/2020/02/D2.1-Governance-Structure-final-Submitted.pdf

2,3 Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

Contact

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

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the authors' view and the Commission is not responsible for any use that may be made of the information it contains.