European Cyber Agora Workstream 2

Navigating the EU Cybersecurity Policy Landscape - Conclusions and Recommendations

Context

In recent years, as the EU cybersecurity landscape witnessed a significant increase in cyberattacks and cyberspace has continued to emerge as a domain of conflict between nation states worldwide, cybersecurity has surged to the top of the EU political agenda. Since the beginning of President von der Leyen's mandate in 2019, the European Commission has put forward several legislative initiatives aimed at strengthening the EU's cybersecurity, resilience, and capacity to respond to major threats. These efforts, which include the NIS2 Directive, the Cybersecurity Act, the Cyber Resilience Act, the Cyber Solidarity Act, and the EUCS have enhanced the European regulatory framework's ability to keep up with evolving cybersecurity challenges, by expanding the scope of the EU's cybersecurity rules to include new sectors and entities, and introducing new obligations for both public and private entities.

After a period of intense regulatory activity for the EU in which a considerable amount of cybersecurity legislations were proposed, negotiated and adopted, and ahead of a new European legislature, the time is right to take stock of the progress achieved, and to identify any remaining gaps that would need to be addressed in the next legislative mandate.

Recognizing that such a stock taking exercise requires cross-sector input to be effective, key institutional, industry, and civil society stakeholders convened for two workshops that took place in the beginning of 2024, prior to this year's European Cyber Agora. Their aim was to assess the current EU cybersecurity regulatory environment, debate its shortcomings and blind spots, and to formulate concrete and actionable recommendations for the next European Commission, thus supporting an informed, multistakeholder approach to EU cybersecurity policymaking.

Conclusions

Discussions during the workshops were centered around four main clusters: (1) taking stock of EU cybersecurity initiatives and legislative instruments and (2) cyber diplomacy efforts, (3) implementation, and (4) stakeholder engagement. The EU has several legislative and non-legislative instruments, institutions and agencies at its disposal to implement its 2020 Cybersecurity Strategy, alongside legislation currently in negotiation, such as the Cyber Solidarity Act. Concluded or still in development EU cybersecurity regulations apply to sectors such as finance, energy, critical infrastructure, including healthcare; thematically, the main areas covered by regulation include enhancing resilience and cooperation and information sharing. In addition to legislative initiatives, there exist several collaboration and coordination initiatives, such as the Cyber Security Alert System, the Joint Cyber Unit, CyCLONe, and the C-CERT network.

Additionally, cyber diplomacy has gained momentum and importance as a component of the EU's coordinated action against cyber threats emanating from outside its borders. Ongoing efforts in this area include the implementation of the Cyber Diplomacy Toolbox, implementing the EU Policy on Cyber Defence, strengthening global partnerships, advancing capacity building support to third countries, and expanding public-private partnerships.

Reviewing the existing EU cybersecurity legislation reveals a highly complex regulatory environment and some overlap between different policy files, highlighting the need for greater oversight in developing policies, given their complementary nature. Acknowledging the rapid progress made in the elaboration of EU cybersecurity policy during the current mandate, stakeholders participating in the workshops strongly emphasized the need for EU policymakers to shift their efforts, going forward, on achieving a successful implementation of the recently adopted files.

While stakeholder engagement throughout the legislative process has increased, it was noted that policymakers could greatly benefit from creating more structured and concerted engagement with industry and other third parties given their technical expertise, especially in the implementation phase of cybersecurity legislation, and in the area of threat intelligence sharing.

The importance of enhanced stakeholder involvement in shaping harmonized cybersecurity standards was also emphasized. Cybersecurity certification processes remain opaque and unclear, often including overlapping requirements, which prompts the need for more transparency and guidance from relevant institutions. Skill shortages and financial constraints also represent hurdles in the way of achieving effective and trustworthy cybersecurity standards and certifications.

Proposals for actions and policy recommendations

Recommendations that emerged from the workshops on ways to address the identified challenges faced by the current EU cyber policy framework can be distilled into three thematic areas, relating to implementation, certification, and Cyber Threat Intelligence (CTI).

The key focus of the next European Commission mandate should be the implementation of existing cybersecurity proposals.

- Effective, evidence-based policymaking requires taking into account the impact of current legislation on the cybersecurity sector. As the effects of files such as the NIS2 Directive cannot yet be subject to assessment, given the file has not yet entered the national level implementation phase, policymakers should now focus on delivering a successful implementation phase for this and other key proposals, as well as providing assistance to member states who require it.
- The next European Commission should consider conducting a detailed review of all EU cyber policy to create a comprehensive overview of any overlap between cybersecurity proposals, and of the interplay

between them regarding their scope and obligations. This review can be used to determine whether any further vertical cybersecurity regulation would need to be developed at a later stage, to complement existing horizontal regulation such as the Cyber Resilience Act.

- Policymakers should maintain regular dialogue with industry to get a detailed understanding of what the challenges are in implementation, and issue guidance accordingly.

The EU should work to strengthen cooperation and increase transparency in its cybersecurity certification framework.

- The value of certification in cybersecurity regulation cannot be underestimated, given its role in building trust and security in products and services. The EU should work to increase transparency of the technical and political processes behind the development of its certification framework, to the benefit of all stakeholders involved. This would ensure that the expertise of standardization bodies is allocated efficiently, and ensure a prioritization in the development of certification schemes based on market needs.
- Cooperation and public-private partnerships are crucial for certification, therefore the EU should work towards more integration of CyCLONe and European cybersecurity certification groups, which, at the same time, should deepen their cooperation with industry.

The EU should consider formulating a clear Cyber Threat Intelligence (CTI) Policy Strategy.

- The EU should take the learnings from the success story of efficient threat intelligence collaboration in the context of the war in Ukraine and develop a consolidated CTI Policy Strategy. The current EU approach to threat intelligence remains fragmented, relying on national strategies that involve a bottom-up patchwork of inputs, which vary greatly between Member States. In order to achieve more effective intelligence sharing, the EU should attempt to scale CTI policy beyond the national level.
- Seeing as there is currently great variation in the approaches to CTI between different Member States, companies, and institutions, the EU should consider establishing a geopolitical cybersecurity platform, similar to the Joint Force Headquarters-Department of Defense Information Network Operations Center (JDOC) in use in the United States, to facilitate information sharing.