European Cyber Agora

# ECA Brussels Communiqué 2022

This year, the European Cyber Agora community is meeting at a critical time. The conventional and hybrid war in Ukraine, geopolitical disruptions in other parts of the EU neighborhood, reinvigorated transatlantic relations, and the return of global power politics in an increasingly multipolar order require the EU to reassess its foreign and security policy, with spillovers in all domains, including cybersecurity.

## Our commitment to multistakeholder engagement that advances European positions on the global stage

1. The European Cyber Agora builds on the objectives of the EU Cybersecurity Strategy 2020, which seeks to increase the resilience and technological development of Europe, build operational capacity to prevent, deter and respond to cyberattacks and advance a global and open cyberspace. We believe these objectives strengthen the position of the EU on the challenges faced by digital societies. We welcome the EU's commitment to global leadership on a wide spectrum of measures addressing current and future cybersecurity challenges.

2. The European Cyber Agora aims to contribute to the ambitions of the EU in cyberspace based on a multi-stakeholder approach. This is outlined in the May 2022 Council Conclusions on the development of the European Union's cyber posture. We pursue this mission by serving as an inclusive platform for regular, structured multistakeholder engagement helping to advance European positions on the global stage.

The European Cyber Agora is implemented by The German Marshall Fund of the United States (GMF), Microsoft and the EU Cyber Diplomacy Initiative (EU Cyber Direct) and is supported by more than 20 partners.

## Our vision for a platform that reflects on the EU cybersecurity agenda against global geopolitical shifts

3. We acknowledge the European Union continues to establish itself as a leading global actor on digital regulation. Similarly, the EU continues to expand its impact on non-legislative discussions on technology, in particular cybersecurity. Be it on internally driven efforts such as enhancing the EU's operational resilience or foreign policy driven efforts like advancing roles of responsible state behavior in cyberspace. As part of this plan, the EU holds a wide array of options to collaborate with civil society, the private sector and other stakeholders to increase its impact even further.

4. As the 2020 Cybersecurity Strategy, the Foreign Affairs Council discussion on technology and foreign policy in July 2021, the Strategic Compass adopted in March 2022 and the Council Conclusions from 23 May 2022 indicate; a secure cyberspace is of growing importance to the EU and the broader multistakeholder community. The war in Ukraine has demonstrated the urgency of more geopolitically-driven discussion and the European Cyber Agora intends to contribute to these discussions via a multi-expertise platform.

5. Events in Ukraine have raised questions and lessons on technology as a foreign policy issue, from sophisticated cyberattacks to the role of open-source intelligence in military planning or foreign interference and information operations. Furthermore, the war has also exposed the reality of a world increasingly ideologically and physically digitally divided. Governments, private companies (not least the tech industry) and civil society can no longer claim neutrality but are contributing to the promotion of shared values in defense of democracy and a rules-based order against a backdrop of growing international polarization. The European Cyber Agora recognizes these trends in cyberspace with deepened reflections around European strategic autonomy and the future of cooperation on the global geopolitical and military stage.

6. This presents both a challenge and opportunity for the EU from a foreign policy perspective. The European Cyber Agora aims to be a platform that supports Europe's ability to lead on setting rules for a digital free world, establishing models to protect democracy from external and internal threats, while ensuring competition and free speech.

## Our dedication to support EU cyber policy making through multistakeholder recommendations

7. To contribute to these discussions, we reiterate our ambition to develop the ECA as a framework that brings together all stakeholders and explores European policy responses to the most pressing issues in cyberspace. Over the past year, the European Cyber Agora has convened its community through Annual Conferences and specialized working groups featuring a program closely aligned to topics relevant to EU objectives. We will also continue to support our community by connecting its stakeholders and advancing their initiatives.

8. In 2021, the Annual Conference highlighted four broad priorities when implementing the EU Cybersecurity Strategy alongside the value of cross-sector input. In 2022, to further elaborate on these areas, key stakeholders of the community convened into working groups with the aim of identifying a relevant focus and to formulate concrete and actionable policy input. Their recommendations are now available[1]:

→ **AREA 1: STRENGHTEN MULTISTAKEHOLDER POLICY INPUT**

**FOCUS: Enhance cross-sectorial lines of communication between stakeholders to strengthen EU leadership in cyberspace.**

9. We note the 2020 Cybersecurity Strategy calls upon the European Commission and High Representative to engage with all stakeholders in cyberspace. The European Cyber Agora creates a platform for new and effective relationships, trust-building and shared policy expertise between EU institutions and the full spectrum of stakeholder groups. Here, the role of academic research to help form an evidence-based EU foreign or cyber policy can still be improved. Measures taken today to form such connections and a trusted work relationship between policymakers and policy researchers will deliver long-term dividends to the EU Cybersecurity Strategy. It will also create positive spillovers for realizing other EU ambitions such as the Joint Cyber Unit. Read the full recommendations of **Working Group 1** in annex.

→ **AREA 2: PROTECT FUNDAMENTAL FREEDOMS IN CYBERSPACE**

**FOCUS: Seek human rights-based approaches and oversight to the market and state use of spyware and other intrusive surveillance technologies.**

10. The illegal use of surveillance software is a growing threat to EU civil rights, with implications for distinct initiatives such as the EU Action Plan on Human Rights and Democracy. We recognize the role of member state legislation, or the 2002 EU e-Privacy Directive, as important legislative instruments to protect those rights. We note the European Parliament's March 2022 decision to launch an inquiry on how to address legal shortfalls and better protect EU fundamental freedoms against the malicious use of intrusive spyware. The European Cyber Agora encourages continuous improvement of civil society and other stakeholders' involvement in this area, especially in co-designing governance mechanisms, as well as continuous oversight of their implementation/function. Read the full recommendations of **Working Group 2** in annex.

→ **AREA 3: IMPROVE PUBLIC-PRIVATE COOPERATION**

**FOCUS: Create a structured dialogue with industry stakeholders, EU institutions and governments around geopolitical and other strategic developments.**

[1] Working Groups were coordinated by GMF and Microsoft. Their conclusions and recommendations generated through this process are a sole responsibility of the authors and do not necessarily reflect the views of other partners of the European Cyber Agora.

11. New initiatives such as the European Cybersecurity Competence Network and Centre demonstrate the EU is taking a proactive, long-term strategic perspective to cybersecurity and cooperation with industry. We welcome the March 2022 EU Strategic Compass and commend its recognition of the role of the private sector in cyber diplomacy and its call for stronger cooperation between the EU and industry players. Sophisticated mechanisms are already in place for the private and public sectors to cooperate on cyber resilience, but conversations about geopolitical implications of incidents, threats and trends is tending to occur only sporadically. Both sides could benefit from having an open exchange in this domain to better understand each other's goals. Platforms such as the Paris Call for Trust and Security in Cyberspace or the Cybersecurity Tech Accord can accelerate this effort. Read the full recommendations of **Working Group 3** in annex.

→ **AREA 4: ADVANCE EU LEADERSHIP IN THE WORLD**

**FOCUS: Strengthen cyber capacity building (CCB) co-operation between the EU and the broad CCB community by adopting a more bottom-up approach.**

12. The May 2022 EU Council conclusions reiterate the need to develop the Union's cyber posture by enhancing its ability to prevent cyberattacks through capacity building and capability development. Today, the large number of CCB actors and projects complicates coordination and implementation. This generates an inherent risk of overlap and duplication. Fostering EU internal coherence, such as creating single points of contact or common indicators, has potential to reduce this risk, with positive impact on CCB efforts, cooperation with third countries, and for initiatives such as the EU Cyber Capacity Building Board. Read the full recommendations of **Working Group 4** in annex.

13. To conclude, the European Cyber Agora, a large and diverse multistakeholder community, stands ready to further support the EU in its cybersecurity ambitions. To address current geopolitical events and the challenges of the future, we will continue to build trust between diverse cyber actors and leverage the growing number of successful best practices in multistakeholder cooperation.