European Cyber Agora

Working Group 4: Advancing a global and open cyberspace

Conclusions and recommendations

Co-leads: Raquel Jorge Ricart, Elcano Royal Institute; David Van Duren, Global Forum on Cyber Expertise; Romain Bosc, The German Marshall Fund of the United States

Context and issues at stake

For years, the European Union has been investing in cyber capacity building (CCB) both internally and externally, either through bilateral or multilateral cooperation. Gradually, the EU has more assertively developed a vision that rests on the promotion of fundamental values such as human rights and the rule of law and a conception of cyberspace as a key driver for global development and prosperity. Major achievements over recent years have contributed to creating important foundations for building cyber capacity both at EU and international levels. The global and multi stakeholder community has played a key role in defining the concept of 'cyber capacity-building', shaping and suggesting frameworks to structure capacity-building efforts and methods to activate and measure their effectiveness.

The European Cyber Agora community has gathered policy experts and practitioners to look at the EU's cyber capacity building (CCB) efforts and to exchange ideas and views on logical next steps in fostering the EU's overarching goal of advancing global and open cyberspace. As acknowledged in the recently released Council conclusions on the development of the EU's cyber posture, the call for the swift establishment of a Cyber Capacity Building Board and regular exchanges in the Horizontal Working Party on Cyber Issues presents opportunity to foster these multistakeholder conversations and strengthen cooperation with existing global and regional coordination networks like the Global Forum on Cyber Expertise (GFCE) and the EU's Cyber Capacity Building Network (EU CyberNet).

Stakeholders from non-profit sectors effectively align with the EU cyber posture's approach to tailored cooperation with EU's external partners. The call to mobilise the Neighbourhood, Development and International Cooperation Instrument (NDICI), the Instrument for Pre Accession Assistance (IPA III), the European Peace Facility (EPF) and the Global Gateway Initiative is advantageous for the entire CCB community.

Identified gaps and shortcomings

One major challenge to overcome stems from the fact that cyber capacity building has evolved within distinct and siloed policy areas and communities. Consequently, the large number of actors and projects across various areas creates complexity and hampers a clear understanding of what actions are needed to ensure effective coordination and implementation. This generates inherent risk of overlap and duplication. While the Working Group welcomed the continued efforts in mainstreaming CCB goals across the entire spectrum of EU policies and instruments, including partnership agreements, it also encourages the EU to build on existing efforts to create more synergies across policy areas and communities.

Proposals for actions and policy recommendations addressed to the EU institutions

Improve coordination by assigning single points of contacts for EU-funded projects on CCB with actors from third countries and establish an inclusive eco-system serving as a common marketplace for the CCB community to work towards the same goals across policy domains and communities.

- Consider the EU Cyber Capacity Building Board as an operational body, able to define objective criteria and identify priority areas for CCB project investments, by ensuring Board members do not overlap or duplicate efforts in their respective DGs, agencies or departments within the EU.
- Provide a one-stop-shop mechanism for sharing information and raising awareness on EU projects and organizations across all policy domains and communities. This will also enable direct match-making and more diversification of stakeholder networks and facilitate access to specific expertise and shorten response timeframes.
- Assign single points of contact – which could be individual experts and/or leading organizations across CCB projects – to improve coordination and facilitate the mainstreaming of CCB goals across the policy agenda.
- Share information on ongoing projects (including relevant actors and used tools) and provide a harmonised catalogue of “curated services” allowing both the EU institutions and stakeholders to identify how any actor can contribute to the missing gaps or emerging demands for incoming projects, EU policy steams and instruments. Build on ongoing ‘mapping’ efforts of, for example, the GFCE community. (http://www.cybilportal.org) and EU CyberNet.

- Showcase best practices and lessons learned from effective project development and implementation in regular meetings, convening the EU with stakeholders altogether. Led by its EU members and partners the GFCE could set up a regular exchange on best practice which could showcase other regions.
- Centralise information and manifestations of interest for new tenders, future projects and funding opportunities. The marketplace would serve as a digital match-making platform and offer stakeholders easy access to potential partners.

Promote a value-based cyberspace through a comprehensive agenda for external action and cooperation with global partners

- Set up meetings with stakeholders to identify potential collaboration in the joint training activities for EU and Member States' staff, as proposed in the EU Cyber Diplomacy Network in the Council conclusions on the development of the EU's Cyber Posture. This will allow both the EU and stakeholders to promote "targeted cooperation" in a much more effective way. Closer cooperation with EU delegations abroad is of interest too.
- Provide more support for the coordination of programmes and expertise at the EU and national levels through the EU CyberNet platform and strengthen support via existing global and regional (multistakeholder) coordination networks facilitated by the GFCE.
- Include the multistakeholder CCB community into the international cooperation efforts as acknowledged by the Council conclusions on EU Cyber Posture, concretely in the Programme of Action (PoA) at the United Nations.
- Promote CCB policy convergence in third countries, especially through existing frameworks, for example the established Africa CCB Coordination Committee (facilitated by the GFCE) and the Digital for Development (D4D) Hub project developed between the African Union and the EU, or extending the scope of Digital Partnership Agreements with Indo-Pacific countries and including new CCB activities.
- Integrate gender equality and inclusion of vulnerable communities into CCB needs analysis, project drafting and implementation mechanisms, cognizant of the need to make cyberspace an inclusive, safe and egalitarian domain for the personal and professional development of all.

Establish common indicators for monitoring countries maturity levels and better assess progress in developing and implementing CCB programmes and goals.

- Remedy the lack of supporting evidence and common assessment methodologies for measuring the effectiveness of CCB initiatives, including key areas such as risk management and performance assessment of national programmes.
- Initiate a process for multistakeholder consultations to define harmonized monitoring and evaluation frameworks, key performance indicators and data gathering practices implemented by the entire CCB community.
- Build upon recent initiatives in this domain, such as those developed by the World Bank, the OECD's Development Assistance Committee (OECD DAC), or Oxford Cyber Security Capacity Centre's Maturity Model to create a comprehensive progress assessment framework. The GFCE's working group on Policy and Strategy could provide the multistakeholder 'place' to facilitate the discussion among these different initiatives.

The European Cyber Agora Working Groups 2022 are coordinated by

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Microsoft

The European Cyber Agora builds on the objectives of the EU Cybersecurity Strategy 2020 and aims to strengthen the ambitions of the EU in cyberspace based on a multi-stakeholder approach. In 2021, the Annual Conference highlighted four broad priority areas when implementing the EU Cybersecurity Strategy alongside the value of cross-sector input. In 2022, key stakeholders of the Agora community convened into four working groups to formulate actionable policy input for each area. The featured recommendations are the output of their consultations and research.