European Cyber Agora

Working Group 1: Enhancing Cross-sectoral Lines of Communication

Conclusions and Recommendations

Co-leads: Jakob Bund, ETH Zurich; Andrea G. Rodríguez, European Policy Centre; Joe Burton, Université libre de Bruxelles

Connecting EU policymakers with policy-oriented academic research outputs is fundamental to continually enhance intelligence-driven and empirically-based EU policies. To strengthen awareness about the communication elements requires this Working Group to focus on two important questions: What means are there to ensure that research insights support cyber policy decisions? And how can cyber policy inform the direction of research?

Recognizing the value of knowledge exchanges between the EU institutions and a wide array of stakeholder groups, this Working Group has focused on identifying and outlining opportunities for the European cyber policy research community.[1] Other sectors and civil society groups stand to benefit from parallel efforts exploring how their interactions with EU policy processes and communications with policymakers might be strengthened.

The Working Group found that policy-oriented research can be most valuable to decision-making when it follows four principles. To facilitate uptake, research findings and ideas need to be:

- **Targeted:** *providing analysis on a well-defined issue*
- **Relevant:** *informing and engaging with strategic priorities*
- **Accessible:** *tying analysis of longer-term strategic challenges to present day-to-day policy challenges*
- **Translatable:** *outlining pathways for integrating analytical insights into policy*

To develop the full potential of these principles, an iterative process that facilitates confidence-building between policymakers and policy researchers is crucial. Measures taken today to build these connections and trusted working relationships will offer long-term dividends. For future policy development cycles, confidence-building efforts could help significantly in leveraging analytical insight because foundations such as these cannot be fast-tracked.

[1] Deliberations of this Working Group were supported by two round table discussions convening stakeholders from the EU institutions, European academic institutions, and, think tanks. The Working Group's recommendations were submitted to participants of these workshop sessions for feedback.

Recommendations developed by this Working Group build on the strength of previous initiatives - leveraging synergies and avoiding duplication. In the spirit of the Open-Ended Working Group on the security of and in the use of ICT (OEWG), the proposed ideas aim to support systematic, sustained, and substantive engagement between EU policymakers and the European cyber policy research community advancing mutual understanding about informational needs with the aim of

- Closing current gaps in the feedback loop by highlighting opportunities to structurally strengthen communication links
- Enhancing the mobility of knowledge and facilitating the integration of research into policymaking
- Ensuring policy analysis is informed about strategic priorities and offers practical value
- Highlighting the need to develop momentum for ideas from conception to implementation
- Showcasing pathways for giving impact to insight.

In supporting these aims, the following recommendations seek to incentivize applied research on EU strategic priorities, capabilities, and risk perceptions in relation to the cyber dimension of foreign, security and defense issues.

Establish a Rapid-Response Resource to Leverage Civil-Society Expertise for Cyber Policy

To support the structured engagement between EU policymakers and the policy research community in Europe, the Council, the European Commission and European External Action Service may consider launching an open call for external experts dedicated to the cyber dimension of foreign, security, and defense policy issues.

Taking advantage of the experience gained by EU CyberNet in bringing together a pool of experts for external capacity-building and co-operation with EU partner countries, this appeal would create connections to support the EU's own policy processes. Broadening the scope to include policy projects that strengthen the EU's cyber posture, these specialists would complement and possibly integrate with the expert pool developed by EU CyberNet.

To form a reserve list of specialists in academia and the European think tank landscape, the call for experts seeks to promote awareness about policy analysis that can support the implementation and strategic development of the EU's Cybersecurity Strategy for the Digital Decade.

Most practically, the call offers a platform for an inclusive bottom-up mapping of subject matter experts focused on the analysis of political risk factors. The resulting expert roster aims to identify and incentivize knowledge production around priority projects in the three areas of action pursued by the EU Cybersecurity Strategy.

In this light, the roster might further serve as a stepping stone for issue-specific outreach to collect civil society perspectives to inform OEWG deliberations and foster a shared global understanding of the UN framework of responsible state behavior in cyberspace.

By highlighting and leveraging existing expertise across the European cyber policy research community, the expert roster could serve as on-demand capacity for policy support through the provision of contextual analysis to inform strategic decision-making. The proactive identification of knowledge hubs in key issue areas positions the roster as a rapid-response resource for policy support that can reduce the ramp-up time for the consultation of civil society expertise.

Strengthen the EU's Capacity to Anticipate Threats by Establishing a Permanent Cyber Foresight Unit

The capacity to model future scenarios by understanding emerging threats is necessary to improve the EU's operational capacity to prevent cyber incidents, improve cyber deterrence, respond to cyberattacks, and identify new and emerging threats.

Given that foresight activities are often carried out by parties outside of the EU institutions and/or focus on a much larger geopolitical landscape, the cyber dimension is often overlooked or not investigated thoroughly. A permanent Cyber Foresight Unit (CFU) would be able to increase the Union's resilience by complementing EEAS and ENISA efforts to navigate complex scenarios and anticipate threats. Adding to other foresight initiatives, the CFU would emphasize a diverse composition of stakeholders to challenge conventional wisdoms and avoid groupthink. To inform decisions on trade-offs in further strengthening the Union's resilience, the CFU would explore overlaps between low-probability-high-impact scenarios and priority risks.

For this reason, the Working Group suggests the European Commission and the European External Action Service establish a permanent Cyber Foresight Unit. The Unit should count on multidisciplinary expertise and include the voices of civil society. The Cyber Foresight Unit would be tasked to

1. Map out vulnerabilities and developments
2. Understand emerging threats in cyberspace and the information warfare space
3. Establish possible scenarios and rank their plausibility
4. Investigate wildcards
5. Organize and take part in simulations to better prepare the Union and its member states for major cyber incidents.

Establish an EU Cyber Policy Fellowship to Enhance Links between Academia and EU Policymakers

This fellowship program would bring think tanks and academics working on cyber policy into sustained contact with European policymakers; to help EU policymakers benefit from cyber expertise in European universities and research institutes and build greater policy awareness in the European cybersecurity academic community.

Academics and researchers would be based in EU directorates and agencies in Brussels for periods up to six months, or at ENISA, the Joint Cyber Unit, and other EU agencies with a cybersecurity role. Researchers might also be embedded within parts of the envisioned EU Cyber Diplomacy Network. Similar fellowship opportunities have been implemented successfully in other polities – the UK for example has a program where academics are based in a government ministry or parliamentary committee.[2]

The fellowships would be based on an agreed program of research on topics relating to the formulation and implementation of EU cybersecurity policy as well as structured opportunities for academics to provide advice, strategic guidance, and input into EU policy initiatives. The program could be extended to civil society and industry representatives with relevant expertise to further close cross-sectoral gaps.

Ensuring support and resources to advance the momentum of existing community-building efforts is just as important. Launched in 2022, the fellowship program of the European Cyber Conflict Research Initiative has established a European incubator for cross-sectoral collaboration on cyber policy matters including European professionals from government, civil society, academia, the private sector, and journalism. The fellowship provides a platform for a diverse exchange with EU personnel through field trip activities and the development of an alumni network to foster lasting connections across the cyber policy community.

EU funding for fellowship programs within and outside of the EU institutional framework could help further expand these opportunities.

[2] https://www.parliament.uk/get-involved/research-impact-at-the-uk-parliament/academic-fellowships/

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.