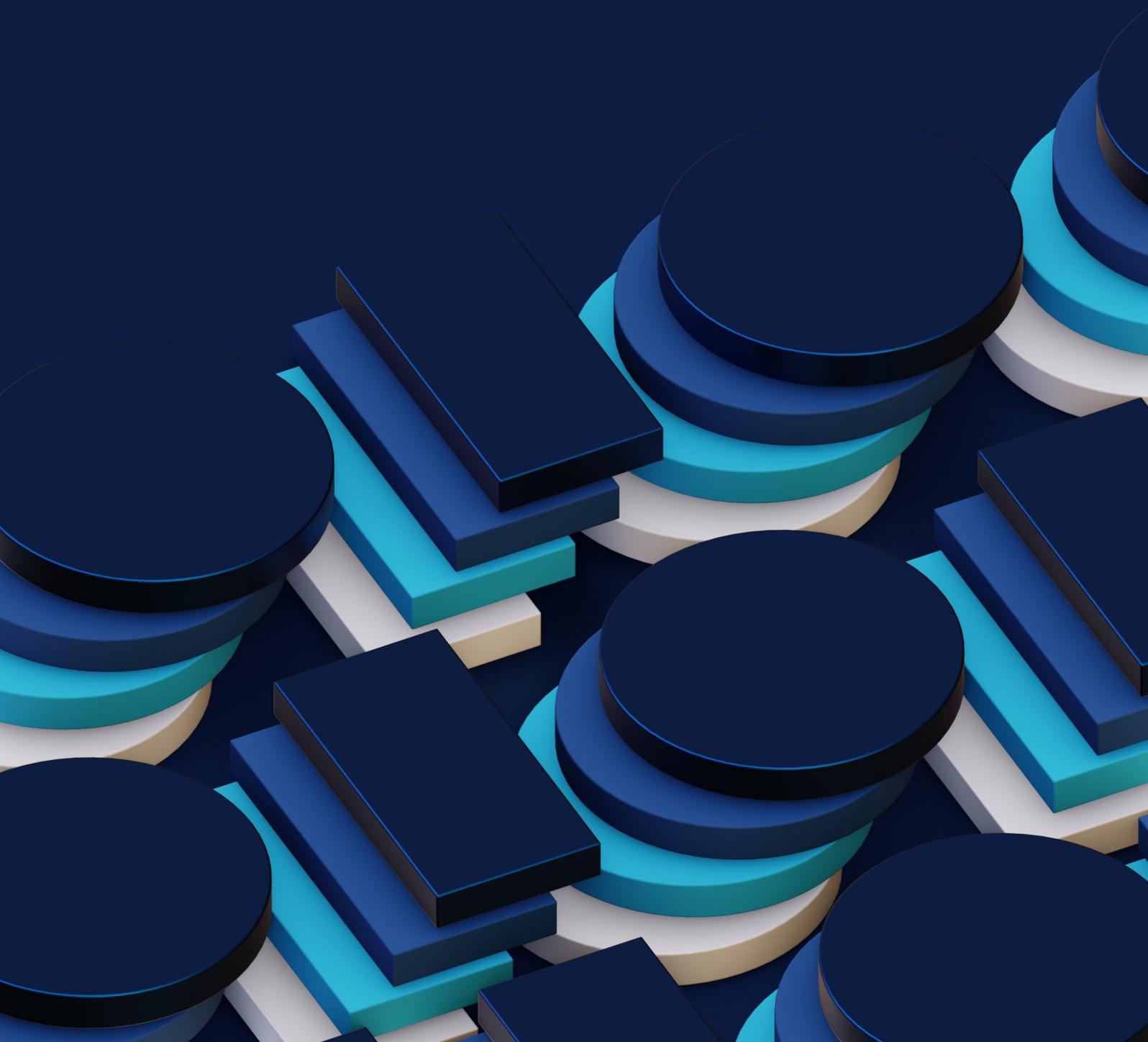


Brussels Communiqué 2022

& Conclusions of the Working Groups



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.

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 available¹:

→ **AREA 1: STRENGTHEN 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.

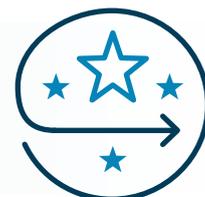


¹ Working Groups were coordinated by GMF and Microsoft. Their conclusions and recommendations generated through this process are a sole responsibility of the authors and do not necessarily reflect the views of other partners of the European Cyber Agora.

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.

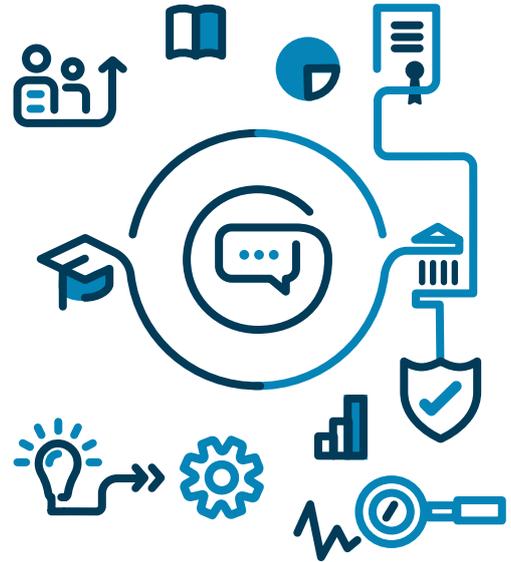
→ **AREA 4: ADVANCE EU LEADERSHIP IN THE WORLD**

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.



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



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.

Working Group 2: Supporting civil society engagement and improving its preparedness

Conclusions and recommendations



Co-leads: Klara Jordan, CyberPeace Institute; Nikolas Ott, Microsoft

Context and issues at stake

There is a growing industry that develops and sells tools, techniques and services enabling their clients, often governments, to break into networks, computers, phones and internet-connected devices. A widespread use of spyware by state and non-state users presents a challenge to the entire digital ecosystem and to those who rely on it, including members of civil society, policymakers, and the technology sector. These stakeholders are at times a target of spyware but also important players in shaping the governance tools to curb this phenomenon. Despite the recent adoption of regulations on dual-use technologies, licensing and export controls, the increasing sophistication and unregulated use of spyware threatens human rights, damages privacy, and undermines trust in technology.

In this context, this European Cyber Agora Working Group on *Supporting civil society engagement and improving its preparedness* explored the role civil society¹ plays in both monitoring the proliferation of these intrusive technologies and shaping a comprehensive response. Through its investigative, consultative, and awareness raising work, civil society has already pushed the topic of spyware into mainstream political discussion.

The Working Group was encouraged to see the creation of the [Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware](#) and further discussion of the topic on the floor of the European Parliament itself. It is also encouraging to see policymakers are beginning to engage with civil society on the topic, with the Inquiry Committee already eliciting testimony from a select few members.

¹ For the purposes of this report, the working group defines civil society as any non-state actor, including, but not limited to non-governmental organizations (NGOs), researchers, academic community, private sector actors, foundations and charitable organizations.

Key insights and identified gaps

Members of this Working Group, including NGOs, private companies, academia and research institutions, agreed that civil society plays a key role across three major areas: awareness raising and education, assistance to victims and advocacy.

Often, policymakers need to gather evidence relying on external and trusted sources to fully grasp an emerging phenomenon. This is particularly true when it comes to technology, as they can lack technical knowledge and awareness of the legal and human rights challenges posed by the use and application of emerging technologies.

Civil society actors are instrumental in alerting decision-makers and society at large, and they have a key role to play in monitoring the evolving spyware market, analyzing its impact and establishing oversight. Awareness raising activities highlighting the effects these tools are having on civilians can bring the issue to the forefront of the debate and prompt a call for a coordinated, global response.

Civil society is already very active in this area; as outlined in Annex mapping the various initiatives and resources ranging from litigations to proposals for legislative and regulatory measures including voluntary initiatives and self-regulation.

As a snapshot, there is continued awareness raising through the investigative research and forensic activities conducted by [Citizen Lab](#) as well as good governance materials such as the [10 Necessary Safeguards](#) against government hacking and surveillance produced by [Privacy International](#) (PI) and the [13 principles](#) by the Electronic Frontier Foundation (EFF). These suggest concrete policy, legal and technical actions to protect users from illegitimate access through legal instruments, new transparency obligations and independent public oversight.

Furthermore, civil society also leads the charge via legal actions to seek redress through the courts, as illustrated through complaints filed by the Electronic Frontier Foundation ([EFF](#)) and Privacy International ([PI](#)) in U.S. and European Courts respectively, as well as through amicus briefs, such as [AccessNow](#), [Amnesty International](#) and others.

Major industry players are also [increasingly vocal](#) on the emergence of a growing grey market for “cyberweapons” developed by private-sector offensive actors (PSOAs) and are calling for more international cooperation on this issue. Microsoft [provided recommendations](#) for greater transparency and oversight of cyber mercenary business practices.

Collaboration across governments, civil society and the private sector is essential to establishing good practices and producing resources to better track and respond. While varied, these current initiatives represent a patchwork of efforts with various levels of implementation. As we witness the continued abuse of the technology, it is evident more needs to be done.

Main conclusions and recommendations towards the global multi-stakeholder community



Policymakers can benefit from creating more structured, concerted engagement with civil society organizations and industry to collect evidence and better understand the market evolution, widespread use, and who the players are behind the development of spyware technologies.

Civil society groups and organizations, as diverse as they are, can provide up-to-date and in-depth analysis of the spyware market, as illustrated in detailed reports on incidents by Citizen Lab, or [in-depth research](#) provided by the Atlantic Council.

These inform the debate and present policymakers with the necessary evidence to:

1. Remedy the lack of transparency;
2. Help understand the diversity of cyber offensive capabilities including spyware;
3. Demonstrate how these technologies are evolving but also the challenges posed by the growing 'Access-as-a-Service' industry as a whole;
4. Better understand the structure and ramifications of the market, the people developing and selling these tools and the various groups and governments involved in their use and proliferation, in order to provide a more effective response.

Policymakers, especially those working towards solutions in the European Parliamentary Inquiry Committee, but also at national level, can benefit from the expertise with civil society and industry. Engaging with the broader multistakeholder community in order to receive technical support, impact assessments, proposals on human rights safeguards and other input can only support the creation and implementation of more effective governance mechanisms.

Industry also plays multiple key roles in prioritizing the security of services and products for users while proactively tracking malicious players and [working with civil society](#) to share insights into the operations and impacts they have on society at large. They can also solidify coalitions with other industry players with shared concerns, draft technical and policy positions and importantly, enhance strategic relationships across civil society and identify avenues for further cooperation.

Civil society can endeavor to provide policymakers with an in-depth overview of the largest current knowledge gap: an analysis of the scope, actors involved, and functioning of the spyware market. This action however requires additional support from policymakers in the form of information as well as operational and potential resource support.



Civil society organizations – including NGOs and industry – play a critical role in providing technical and legal assistance to victims, and operationalizing solutions on the ground.

An important role for civil society is to act as “watchdogs” and provide technical and legislative assistance to victims. Their critical role resides in their ability to identify targets of intrusive surveillance techniques, notify them and pass their cases along to investigative organizations. They also provide information and assistance governments can leverage in designing effective and future-proof policies. Civil society organizations also have a role to play in collaborating with technology companies to improve business processes or products and increase their resilience against exploitation by malicious actors.

Furthermore, civil society actors contribute to the development of good governance models that in turn, can be used by groups such as development agencies. Also, civil society organizations have a role in educating vulnerable groups on methods of protection and in distributing training/ materials to ensure good cyber hygiene and resilience against intrusion. To this end, this group supports the overarching EU’s cyber capacity building strategy and stresses the role of civil society organizations in building collective capacity to identify and address cyber threats as well as to investigate and prosecute cybercrimes.

Industry players are making an important contribution in this field using their technical capabilities and experience in shaping public policy. For example, the Microsoft Threat Intelligence Team (MSTIC) tracks actors in this space and has developed strong technical relationships with key civil society personnel in this area. This has, amongst other things, led to the disruption of [Sourgum](#) in 2021, when Microsoft published a detailed overview of the techniques and exploits used in that particular case.

Microsoft also supported WhatsApp by filing an [amicus brief](#) in its case against the NSO Group. Other private actors have also played a proactive role in mitigating the effects of these groups. [Apple](#) filed a lawsuit against the NSO Group and its parent company holding it accountable for the surveillance and targeting of individuals. The company’s statement commended groups like the Citizen Lab and Amnesty Tech for their groundbreaking work towards identifying cybersurveillance abuses and helping to protect victims.

In addition to this, Meta recently took [action](#) to disable several entities targeting people across the world online. The company followed up by sharing the findings with security researchers, other platforms and policymakers, issued ‘Cease and Desist’ warnings and also alerted people believed to be attacked so they could strengthen the security of their accounts.

In addition to that, ESET experts indicate that ESET Mobile Security offers an [effective protection](#) against the Pegasus software for Android devices. Apple iOS users can also check if their smartphones have been hacked. These and multiple other positive examples outline the synergies and points of cooperation between the multistakeholder community in tackling the illegal use of spyware.



increase transparency and accountability on the spyware market, policymakers would benefit from working closely with civil society in designing and implementing effective governance, oversight and regulatory measures. Main proposals for consideration include:

- The role investors can play in overseeing the practices of spyware companies they fund such as proposed in the [Human Rights Due Diligence Guide for Investors](#);
- The use of Access to Information laws in order to gain transparency into state purchases/ use/export of spyware technologies;
- The potential for regulation on government transparency and disclosure of vulnerabilities;
- Civil and criminal litigation against companies selling and operating spyware;
- The role of state-led national investigations into the deployment of spyware;
- Robust implementation of due diligence clauses in dual-use regulations;
- Implementation of the [Checklist for Accountability in the Industry Behind Government Hacking](#).

Towards this aim, the Working Group has assembled additional materials in the Annex including a visual mapping of current initiatives and civil society contributions, an overview of the policy instruments and proposals, as well as some major private sector actions, all aimed at bringing about solutions to this complex and borderless challenge.

While these are encouraging developments, there is still room for more active engagement and positioning by European policymakers; for instance, by taking concrete action toward enhancing trust in technology. With improved coordination, the multi-stakeholder community can withstand the challenge of increasingly sophisticated surveillance technology.

The European Cyber Agora Working Groups 2022 are coordinated by



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.

Annex: Core Material

Pages 16 - 22

European Cyber Agora

Working Group II



Supporting civil society's engagement and improve its preparedness

Intrusion Software

A European Policy and Operational Toolbox



A summary of **existing instruments** and the implementation status of policy measures

Disclaimer: the following provides an in depth, albeit non-exhaustive, overview of the policy landscape

	Measure	Target	Scope	EU Implementation	Beyond EU Implementation	Instrument(s)
(L)	National Legal Frameworks	State (LEA)	Governing the use of surveillance technology by state actors against their citizens (i.e. what procedures must be followed)	■ None		<ul style="list-style-type: none">National LegislationEuropean Convention on Human RightsInternational Covenant on Civil and Political RightsEU Charter of Fundamental Rights
	Moratorium/Ban	State Company	Completely halting the trade, sale, export, and usage of intrusive surveillance technology by states	■■■ Existing proposal (EU DPA)		<ul style="list-style-type: none">Not Applicable
	Criminal Action	Company Individual	Holding Executives criminally responsible for violations of human rights through the unlawful use of their technology	■■■■■ Implemented (Genocide NetworkK)	Implemented in US with the Alien Tort Statute	<ul style="list-style-type: none">National LegislationRome StatuteUN Guiding Principles on Business and Human Rights
	Civil Action	Company	Bringing suits against companies to seek civil damages for violations of rights	Not Applicable		<ul style="list-style-type: none">National LegislationUN Guiding Principles on Business and Human Rights
(R)	Sanctions	State Company	Banning the export of dual use technology with surveillance purposed to states who are geo-politically opposed/known to violate human rights	■■■■■ Implemented (global human rights regime)		<ul style="list-style-type: none">National Legislation
	Export Controls	Company	Regulating the export of dual use technology with surveillance purposes to those who may abuse the technology	■■■■■ Implemented (2021/821 dual-use items export control regime)	Implemented in 42 states (Wassenaar Arrangement)	<ul style="list-style-type: none">National LegislationWassenaar Arrangement
	Mandatory Reporting / Due Diligence	Company	Reporting to judge the business practices of companies involved with the surveillance technology sector	■■■ Directive adopted (2022/0051 corporate sustainability due diligence)	US Draft Guidance (for the Export of Hardware, Software and Technology with Surveillance Capabilities...)	<ul style="list-style-type: none">National LegislationUN Guiding Principles on Business and Human RightsOECD's Guidelines for Multinational EnterprisesOECD's Due Diligence Guidance for Responsible Business Conduct
	Public Mechanisms for Approval and Oversight	State	Public approval mechanism to regulate the purchase/export/use of surveillance technology	■ None	Sporadic local implementation	<ul style="list-style-type: none">National LegislationUN Special Rapporteur on freedom of expression recommendation
(S)	Voluntary Due Diligence / Transparency Mechanisms	Company	Voluntary reporting to analyze the human rights impacts of a company's business activities	Not Applicable		<ul style="list-style-type: none">UN Guiding Principles on Business and Human RightsOECD's Guidelines for Multinational EnterprisesOECD's Due Diligence Guidance for Responsible Business Conduct
	Corporate Ethics Committees	Company	Analyzing business activities and potential customers against human rights	Not Applicable		<ul style="list-style-type: none">UN Guiding Principles on Business and Human Rights

Civil Society * policy and operational contributions relating to intrusion software

** For the purposes of this workshop, the working group defines **civil society** as any non-state actor, including, but not limited to non-governmental organizations (NGOs), researchers, academic community, private sector actors, foundations and charitable organizations.*

Disclaimer: the following provides an in depth, albeit non-exhaustive, overview of civil society's contribution in this space.

Measure	Current Civil Society Recommendations	Civil Society Involvement
National Legal Frameworks	<ul style="list-style-type: none"> ● Guideline produced by Privacy International to map the components of legislation that can meet rights standards. 	<ul style="list-style-type: none"> ● Privacy International has contributed guides and information to be used for the implementation of effective policy, and has been involved in numerous legal challenges to combat laws not in line with rights standards (Example). ● Electronic Frontier Foundation has similarly created a Necessary and Proportionate coalition that works to ensure democratic oversight and responsible use of surveillance tech. ● Citizen Lab and Amnesty International recently gave expert testimony in hearings at the Inter-American Commission on Human Rights concerning the use of spyware in El Salvador. ● Human Rights Watch, Access Now and others have pushed a call for Indian Authorities to independently investigate abuses of surveillance technology.
Moratorium/Ban	<ul style="list-style-type: none"> ● Numerous calls supporting moratorium from media and civil society. 	<ul style="list-style-type: none"> ● A group of civil society actors put together a call echoing that of the rapporteur calling for a moratorium until sufficient human rights safeguards are in place.
Criminal Action	<ul style="list-style-type: none"> ● FIDH has recommended working to eliminate barriers to justice that arise from issues of jurisdiction and providing greater access by limiting financial and practical barriers for those seeking justice. 	<ul style="list-style-type: none"> ● FIDH brought a case against executives of Amesys/Nexa within French Courts. ● EFF brought a case against DarkMatter executives in US courts. ● EFF supported a case brought by Chinese nationals against Cisco for aiding and abetting in human rights violations.
Civil Action	<ul style="list-style-type: none"> ● FIDH has recommended working to eliminate barriers to justice that arise from issues of jurisdiction and providing greater access by limiting financial and practical barriers for those seeking justice. 	<ul style="list-style-type: none"> ● Apple brought a case against NSO Group in 2021 to hold it accountable for the surveillance and targeting of Apple users. ● Meta brought a case against NSO Group in 2019. ● FIDH has provided recommendations.
Sanctions		<ul style="list-style-type: none"> ● Joint civil society call for the EU to impose human rights bases sanctions against NSO Group
Export Controls		
Mandatory Reporting / Due Diligence		<ul style="list-style-type: none"> ● EFF provided comments to the US State Department's proposal for mandatory human rights due diligence reporting for the export of dual use technology.
Public Mechanisms for Approval and Oversight	<ul style="list-style-type: none"> ● Microsoft provided recommendations for greater transparency and oversight of cyber mercenary business practices. 	<ul style="list-style-type: none"> ● Examples include local organizations, like S.T.O.P. in New York, drafting and organizing support for legislative initiatives and eventually participating in oversight consultations. ● EFF and Oakland Privacy drafting and supporting legislation in Oakland CA and many others, mostly across the United States. ● Microsoft drafted an initial high level policy position and response to the UN Working Group on the Use of Mercenaries. ● Meta encouraged the governments to begin to draw attention to this threat and take action against it.
Voluntary Due Diligence / Transparency Mechanisms	<ul style="list-style-type: none"> ● EFF provided recommendations that voluntary reporting and policies are not the most effective and should be made mandatory through a variety of mechanisms, including mandatory due diligence for export. 	<ul style="list-style-type: none"> ● EFF Recommendations
Corporate Ethics Committees	<ul style="list-style-type: none"> ● Atlantic Council recommends this action and encourages the US to make the existence of an ethics committee a requirement for awarding government procurement contracts. 	<ul style="list-style-type: none"> ● Atlantic Council Recommendations
Multistakeholder Collaboration		<ul style="list-style-type: none"> ● Microsoft discussions on DarkMatter and contravening of “no offense” pledge made through the Cybersecurity Tech Accord. ● Microsoft, Google, Cisco, and VMWare supported WhatsApp by filing an amicus brief in support of Meta’s lawsuit. This led to the establishment of a working group on the topic within the Cybersecurity Tech Accord. ● Meta disabled seven entities who targeted people across the internet in over 100 countries ● ESET Mobile Security developed as an effective protection against Pegasus for Android devices.
Developing Secure Technologies		
Research and Investigations		<ul style="list-style-type: none"> ● Microsoft published a detailed overview of the techniques and exploits used by Sourgum in 2021.

Working Group 3: Enhancing Collaboration between the Tech Industry and European Governments

Conclusions and recommendations



Co-leads: Thomas Boué, BSA Software Alliance; Andy Garth, ESET; John Hering, Microsoft, Eneken Tikk, Cyber Policy Institute

The interconnected nature of cyberspace requires joint efforts to maintain a global, open, stable and secure cyberspace.¹ The European Union (EU) seeks to promote inclusive engagement where governments, civil society and the private sector, work together.² Reinforcing regular and structured exchanges with stakeholders is one of the EU strategic cybersecurity initiatives.³ The Council has recently concluded that strengthening ties with the private sector would amplify the EU's ability to protect and promote a unified vision of cyberspace based on shared values and democratic principles.⁴

To build towards effective cooperation between governments and industry, this Agora Working Group sought to identify areas where governments and ICT industry share the same values and objectives, and thus may offer avenues for closer collaboration. The co-leads of this Working Group⁵ believe tapping into the full potential of multistakeholder cooperation would require strategic alignment between cybersecurity stakeholders; an alignment that would not only create flexible and dynamic cooperation mechanisms and options but acknowledge shared values as well as benefits to be achieved together.



1 – ICT industry shares the vision of an open, free, global, interoperable, reliable, and secure Internet

The Euro-Atlantic vision of an open, free, global, interoperable, reliable, and secure Internet⁶ is shared by many members of the digital industry across the world providing information and communications infrastructure, connectivity, Internet services, ICT hardware, applications, cybersecurity products and services as well as digital marketplaces and social exchange platforms.

¹ The EU's Cybersecurity Strategy for the Digital Decade, page 22: To advance multi-stakeholder cooperation on cybersecurity issues, the Commission and High Representative, in line with their respective competences, aim to reinforce regular and structured exchanges with stakeholders, including the private sector, academia and civil society, underlining that the interconnected nature of cyberspace requires all stakeholders to exchange upon, and take their specific responsibilities to maintain a global, open, stable and secure cyberspace. These efforts will provide valuable input for potential key actions at EU level.

² 2030 Digital Compass: the European way for the Digital Decade.

³ The EU's Cybersecurity Strategy for the Digital Decade, page 23.

⁴ Council conclusions on the development of the European Union's cyber posture, 23.05.22, para 13.

⁵ The co-leads of Working Group 3 are Eneken Tikk, Senior Research Lead, Cyber Policy Institute (CPI), Andy Garth, Government Affairs Lead, ESET, John Hering, Senior Government Affairs Manager, Microsoft and Thomas Boué, Director General, BSA Software Alliance.

⁶ Declaration for the Future of Internet.

To take public-private partnerships to the next strategic level, it is essential to acknowledge the aspirations and directions that stakeholders share and recognize the differences that industry and governments have. For instance, successful implementation of regulatory frameworks like the NIS Directive requires different, yet complementary, contributions from governments and industry. Different perspectives from industry and governments have contributed to strengthening the security of 5G networks. Together, governments and industry can advance policy frameworks like the EU Cyber Diplomacy toolbox.

The ICT industry is instrumental in creating open societies, driving societal change and advancing democratic values. Operating across the world, the tech industry has more responsibility in promoting peace, security and democracy today than ever before, as society becomes ever more reliant on technology to operate. Where governments set the rules, industry must respond and implement these in a proactive and sustainable way. In particular, the tech industry is on the frontline to uphold high standards of privacy and freedom of information, advance corporate responsibility, human rights, and fundamental freedoms and is taking proactive actions to accelerate the green and digital transitions and address the digital divide.

A prime example of this is how for over four years now, the [Cybersecurity Tech Accord](#) – a commitment of more than 150 companies to improving the security, stability, and resilience of cyberspace – has been advancing cyber hygiene principles and the adoption of [vulnerability disclosure](#) policies by technology companies. Signatories have also [been vocal](#) on the need for multistakeholder inclusion in the UN cybersecurity dialogues, and recently shared [more insights](#) on the role and responsibility of technology industry in the age of hybrid warfare. In the same vein, and against a backdrop of cyberattacks increasingly targeting essential services and infrastructures such as hospitals and energy facilities, a group of CEOs from oil and gas company [pledged](#) to enhance cyber resilience across the entire supply chain.



2 – ICT industry shares the goal of reducing the threats and risks in cyberspace

The ICT industry has witnessed, responded to, and mitigated against the threats and risks outlined in recent EU policy documents first-hand. Malicious and hostile cyber actors can exploit and erode trust in digital products and services. It is in the interest of both industry and government to share a high-level of awareness to understand the evolution and advancement of threats and threat actors who use ICTs for harmful purposes. Cyber related policy making must consider the realities of mitigating attacks and the process of response to contribute to cybersecurity ecosystems.

Recent examples illustrate how enhanced public-private collaboration can help in tackling cyber incidents and mitigate risks. In the context of the war in Ukraine, major cybersecurity firms have provided operational support to the Ukrainian government by moving key functions into a secured cloud environment. Leading European cybersecurity firms [have collaborated](#) with national

authorities and provided threat intelligence and information on ongoing cyberattacks targeting critical infrastructures. Industry's [threat assessments](#) and trend observations complement the understanding of harmful ICT practices, while awareness raising campaigns help reduce their costly impact, for instance on risks [posed by ransomware](#) to organizations and users.



3 – ICT industry contributes to government efforts to maintain international peace, security and stability in cyberspace

Providing peace, security and stability primarily remains the responsibility of governments. However, enhancing cybersecurity and increasing resilience requires functioning public-private partnerships. Sustainable digital development requires the ownership and responsibility of industry and would not be possible without equal and transparent cooperation with governments. The many occasions of such cooperation – in threat intelligence sharing, dismantling botnets, thwarting cyberattacks, patching vulnerabilities and securing supply chains – testify to the shared vision and common concerns between the public and private sector.

In an effort to protect their users and customer base, industry invests substantial resources in developing high-quality digital products and services, including resources to protect its online services. Industry also works with governments and customers to detect, prevent and mitigate threats to their accounts and data. Finally, industry shares interest in [protecting civil society](#) from cyberattacks and their harmful effects.



4 – ICT industry can help shape global rules and standards

The EU has pledged to remain open to all companies complying with European rules and standards in so far as respective players will safeguard European values⁷, fundamental rights and security and are socially balanced.⁸ Industry shares the goals of connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms outlined in the Declaration for the Future of Internet. It is in the digital industry's and European governments' mutual interests to shape global rules and international standards in the field of ICTs.

Industry can be instrumental in this and increase the EU's competitiveness and resilience through standardization.⁹ For instance, the [5G Infrastructure PPP](#) works to have European industry driving the development of 5G standards and to develop and exploit at least 20% of the 5G standards essential patents. Also, the Coalition to Reduce Cyber Risk (CR2) *encourages government*

⁷ See Press Release: EU and international partners put forward a Declaration for the Future of the Internet, Brussels, April 28, 2022; Press Release: Commission puts forward declaration on digital rights and principles for everyone in the EU, Brussels, January 26, 2022; https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2695. As of June 1, 2022, the Declaration of the Future of the Internet has been signed by 28 states in addition to the EU Member States and the United States. See <https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet>. These states have pledged to be united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. They promise to welcome all partners who actively support a future for the Internet that is open, free, global, interoperable, reliable, and secure.

⁸ Conclusions of the European Council of 1 and 2 October 2020.

⁹ An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market, COM(2022) 31 final (Brussels, 2.2.2022).

regulators from all countries and all sectors of the global economy to leverage best-in-class international standards, such as ISO/IEC 27101 and ISO/IEC 27103, as the starting point for their approach to cybersecurity.”¹⁰

Conclusions and way ahead

Mutual reliance, trust and cooperation between European governments and digital industry has never been more pertinent. We invite the EU to open a regular, encompassing dialogue and engagement base with industry. A strategic public-private partnership, one driven by shared goals and aspirations will help mitigate against differences that governments and industry, in their respective roles and perspectives, may have. The many processes in which governments and industry work together¹¹ demonstrate cooperation is already possible within defined and specific goals and intentions. The promotion of a value-based policy agenda able to shape technological development but also to address the fragmentation of the policy landscape and balkanization of cyberspace, is a priority for both parties.

By treating the public-private partnerships on an *ad hoc* basis or focusing on formalized collaboration only on technical/operational matters, both industry and governments miss opportunities to achieve shared goals and aspirations. While governments hold the mandate on security and set the rules in the public interest, industry needs to be able to adapt its operations and develop optimal market solutions alongside effective technical standards. An open and balanced dialogue is needed at both strategic and technical level to ensure trust and mutual reliance. Areas such as innovation, education, and skills development are also requiring enhanced public-private collaboration and a common approach towards shared goals and aspirations.

The way the private sector and governments have worked together to address the most pressing recent health and geopolitical conflicts are testament to the wide scale cooperation that is necessary and possible to solve new global challenges. Governments and industry need to build a higher level of trust and confidence, mutual understanding of the environment and goals they could serve. It is in the joint interests of government and industry to overcome the digital divide and prevent further destabilization of cyberspace. The potential benefits of mutual understanding and acknowledgment between governments and industry are many but trust, cooperation, equality, mutual accountability, and transparency is also required.

¹⁰ Coalition to Reduce Cyber Risk White Paper on Seamless Security, 26 February 2020; <https://www.crx2.org/seamless-security-white-paper-press-release>

¹¹ European Cybersecurity Organization, Paris Call Community, the European Cyber Agora, UN OEWG and Cybercrime Treaty consultations etc.

The European Cyber Agora Working Groups 2022 are coordinated by



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.

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 streams 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



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.

Please direct inquiries to:

The German Marshall Fund of the United States

Residence Palace, Rue de la Loi 155

1040 Brussels

T +32 2 238 52 70

