European Cyber Agora

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 society[1] 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

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.

Annex:
Core Material

European Cyber Agora

Working Group II

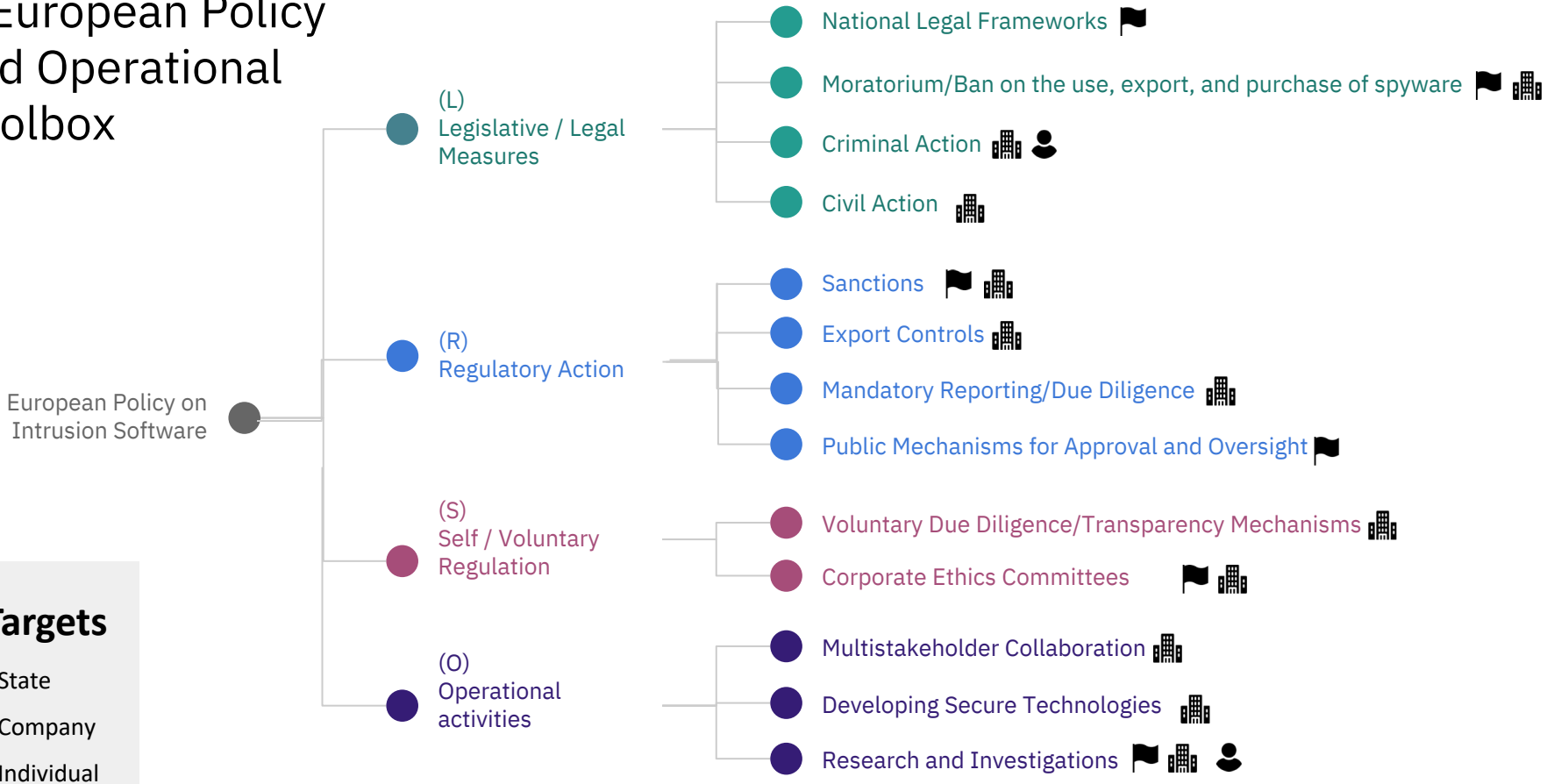
CyberPeace Institute

Supporting civil society's engagement and improve its preparedness

@2022 CyberPeace Institute all rights reseved

Intrusion Software

A European Policy and Operational Toolbox



@2022 CyberPeace Institute all rights reseved

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

@2022 CyberPeace Institute all rights reseved

	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**		• National Legislation • European Convention on Human Rights • International Covenant on Civil and Political Rights • EU 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)		• Not Applicable
	Criminal Action	Company Individual	Holding Executives criminally responsible for violations of human rights through the unlawful use of their technology	■■■■■ **Implemented** (Genocide NetworK)	Implemented in US with the Alien Tort Statute	• National Legislation • Rome Statute • UN Guiding Principles on Business and Human Rights
	Civil Action	Company	Bringing suits against companies to seek civil damages for violations of rights	Not Applicable		• National Legislation • UN 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)		• 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)	• National Legislation • Wassenaar 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...)	• National Legislation • UN Guiding Principles on Business and Human Rights • OECD's Guidelines for Multinational Enterprises • OECD'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	• National Legislation • UN 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		• UN Guiding Principles on Business and Human Rights • OECD's Guidelines for Multinational Enterprises • OECD's Due Diligence Guidance for Responsible Business Conduct
	Corporate Ethics Committees	Company	Analyzing business activities and potential customers against human rights	Not Applicable		• 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 c**ivil 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.

@2022 CyberPeace Institute all rights reseved

Measure	Current Civil Society Recommendations	Civil Society Involvement
National Legal Frameworks	• Guideline produced by Privacy International to map the components of legislation that can meet rights standards.	• 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	• Numerous calls supporting moratorium from media and civil society.	• 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	• 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.	• 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	• 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.	• 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		• Joint civil society call for the EU to impose human rights bases sanctions against NSO Group
Export Controls		
Mandatory Reporting / Due Diligence		• 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	• Microsoft provided recommendations for greater transparency and oversight of cyber mercenary business practices.	• 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	• 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.	• EFF Recommendations
Corporate Ethics Committees	• Atlantic Council recommends this action and encourages the US to make the existence of an ethics committee a requirement for awarding government procurement contracts.	• Atlantic Council Recommendations
Multistakeholder Collaboration		• 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
Developing Secure Technologies		• ESET Mobile Security developed as an effective protection against Pegasus for Android devices.
Research and Investigations		• Microsoft published a detailed overview of the techniques and exploits used by Sourgum in 2021.

@2022 CyberPeace Institute all rights reseved