EVENT SUMMARY

Europe regional consultation: strengthening effective and inclusive cybercrime policymaking

January 2022

Contents

Background

In 2022, and following the United Nations (UN) General Assembly Resolution 74/247,[1] member states begin negotiating a possible new convention on countering the criminal use of ICTs in the UN Third Committee. Given the significance of this process and the impact that a new international treaty might have on international cooperation in this domain, it is important that this process promotes a human-centric approach and adopts a transparent and inclusive model of engagement with diverse group of stakeholders. These stakeholders must be representative of all sectors and communities around the world affected by cybercrime – including women and marginalised groups – and well-informed on key issues and developments.

On 10 November 2021, Chatham House and the EU Cyber Direct Project virtually convened a regional consultation to engage with non-state stakeholders from the wider European region, with the aim of providing them with a platform to share their perspectives on developing a new international convention on cybercrime.

The session welcomed over 45 representatives from civil society, academia, research institutions, the technical community and private sector. Participants were divided into three breakout sessions addressing key areas: scope and criminalization; procedural measures and human rights safeguards; and international cooperation (including harmonisation and fragmentation). The consultation started with a scene-setting plenary followed by the breakout rooms. To close the consultation, participants re-convened in the plenary to share some key takeaways that emerged from the discussions in their respective breakout sessions. The consultation was convened under the Chatham House Rule.[2]

The participants covered a wide range of issues in the breakout sessions and plenary. This summary brief covers some of the key takeaways.

Plenary 1. Scene Setting: The Status of UN Cybercrime Negotiations

The project team presented an overview of the progress that has been achieved within the Ad Hoc Committee so far, including on modalities of engagement agreed in May 2021. The presentation then tackled the positions of member states in response to the AHC Chair's request for submissions on the scope, objectives and structure of a future convention.[3]

Breakout Session 1. Scope and Criminalization

Discussion questions

1. What are the offences that should be included in the new treaty? What should be avoided and why? What are the red lines?
2. How do we ensure compatibility with existing widely accepted international standards, such as the Budapest Convention?
3. How do we ensure that the language of the new treaty is technology-neutral?

[1] A/RES/74/247 - E - A/RES/74/247 -Desktop (undocs.org).
[2] Chatham House Rule | Chatham House – International Affairs Think Tank.
[3] Ad Hoc Committee First Session (unodc.org).

- Participants agreed that the convention needs clear guidelines and terminology to avoid overreaching criminalization. The less precise the language, the more likely it is to be abused. 'CIA' (confidentiality, integrity and availability) crimes will likely be a starting point for the negotiations. Crimes must be defined in **clear and precise terms**, and definitions must strictly follow the principles of **necessity and proportionality**.
- It is also crucial to recognise that the legal, technical and policy terminology of cybercrime may differ between different sectors, disciplines and backgrounds. Recognising terminological differences is critical to overcoming any misunderstandings.
- The scope of criminal activities covered by the UN convention should be defined carefully to **avoid the creation of similar offences covered under different laws** and **avoid duplicating existing efforts or agreements**.
- Given the increasing scope, sophistication and severity of cybercriminal activities targeting critical national infrastructure, participants recognised that **technology-neutral or detached terminology** may help with future-proofing the convention and its implementation over a longer period. Hence, criminalising the activity instead of criminalising the technological form or method used in the commission of the act could be a helpful approach in defining the scope of the convention.
- Reaching an agreement will be difficult because – as evidenced by their submissions – states take different positions on **content-related crimes**. Hence, participants agreed that it is necessary that **human rights standards are embedded in the convention** and that the scope of criminalization follows these standards.
- Participants recognised that criminalization of certain types of content would also lead to **increased pressure on the private sector** to perform takedowns and regulate users with their terms to avoid liability. These practices, especially due to an increasing trend of automation in content moderation, can further impose additional **restrictions on free speech by the private sector**. Furthermore, national interpretations of content crimes can lead to fragmentation of regulatory practices and private industry applying rules from jurisdictions that may restrict speech to users.
- Participants noted that an overreach in criminalization may **weaponise online content against dissidents and activists**, as has been the case with several state practices. When crimes are vaguely equated with content, human rights are on the line.
- Participants disagreed over the merits of the **inclusion of additional protocols** to single out contentious areas related to the scope of criminalization. Additional protocols may help state parties agree to a baseline convention, but they also may create space for abuse of criminalization and legitimise practices that can lead to human rights abuses.

Breakout Session 2. Procedural Measures and Safeguards for Human Rights

Discussion questions

1. What are the adequate domestic procedural measures and criminal procedural provisions regarding mechanisms for cooperation between the parties to the proposed convention, in particular with regard to cooperation in investigations and other judicial proceedings and in obtaining electronic evidence?

2. What elements does a new convention on cybercrime need to have in order to ensure compatibility with human rights and fundamental freedoms, limiting any interference to what is necessary and proportionate for the purpose of specific criminal investigations?

3. Should the new treaty also address minimum standards, including fundamental safeguards, for forensic tools used for the seizure of electronic evidence? What about obligations on non-governmental organisations, such as internet service providers, based in the territory of another state?

- **Human rights safeguards** for researchers, activists, whistle-blowers and other stakeholders must be directly referenced in any future convention. Participants emphasised that these safeguards – which would apply to the convention's substantive and procedural provisions – would help ensure that civil society's activities are not unjustly criminalised or subject to politicisation.
- To ensure that a new convention on cybercrime is **compatible with human rights and fundamental freedoms** – and limits any interference to what is necessary and proportionate for the purpose of specific criminal investigations – participants agreed that the negotiations and provisions in a treaty must be de-politicised.
- A diverse range of non-state actors working collaboratively can help de-politicising by providing evidence-based and expertise-focused assessments of the proposals. Participants referred to the Open-Ended Working Group and Group of Governmental Experts as examples of two processes that, despite high degrees of politicisation, have managed to **bridge differences among states** and resulted in the adoption of two consensus reports.
- Participants agreed that a new convention should encourage **transparency of evidence acquisition tools**, as part of larger efforts towards more transparency when it comes to national cyber capabilities and the importance of doing so for **building trust and accountability**. On a related note, there should be an available framework for accountability in obtaining and retaining data by law enforcement agencies (LEAs).
- Participants also addressed issues of security and privacy for end-users, noting that provides and LEAs must have clear means to **challenge or refuse requests**; however, grounds for refusal must be firmly rooted in and mandated by **human rights obligations**.
- Participants recognised the efficiency of new practices of sharing evidence, such as direct requests to providers. These new practices can considerably speed up investigations, thus **overcoming the challenges associated with mutual legal assistance treaties** (MLATs) in certain instances.
- Nonetheless, MLATs should remain the default, and properly resourcing MLAT assessment teams should be a priority. Granted, some participants noted that principles of **mutual trust alone should not be considered sufficient guarantee** of human rights protections. A new convention should outline provisions or guidance for parties that engage in direct requests outside of MLATs to ensure adherence to human rights standards.
- Participants also noted that the negotiations of a new cybercrime treaty overlap with growing calls for a **global regime on data exchanges**. There is a certain level of uncertainty regarding how discussions about data localisation and data governance might impact future regulation about access to electronic evidence. Participants agreed that a new convention must adopt a mature approach to data exchange for law enforcement purposes. This approach must be realistic about how nations request and obtain data, and the technologies they use to do so, as well as its adherence to states' human rights obligations.
- Finally, some participants mentioned the danger that could arise from states adopting a strong **territorial approach**, as evidenced by the Russian draft proposal.[4] The Russian draft is enshrined in territorial sovereignty, particularly Articles 3 and 46.5, raising questions about **jurisdiction**. Participants expressed

[4] For all submissions to the first session of the Ad Hoc Committee, visit: Ad Hoc Committee First Session (unodc.org).

concerns that an approach like this might significantly impede operational cooperation in investigation and taking down botnets, or by creating ambiguity over how state authorities can access electronic evidence.

Breakout Session 3. International Cooperation and Issues of Harmonisation and Fragmentation

Discussion questions

1. How can the new convention improve international cooperation against cybercrime? What are some of the practical measures it can include to empower national law enforcement authorities?
2. In which ways can a future convention on cybercrime complement the Council of Europe's Budapest Convention and other existing instruments?
3. Conversely, in which ways could a future convention undermine existing instruments? What impact will this have on State parties to those instruments and on the fight against cybercrime more generally?

- Participants recognised the **existing appetite from a number or states for a new convention**, but acknowledged that the convention process will be highly politicised and challenging. There is a possibility member states will not reach an agreement on a convention by the end of the process.
- A good outcome from the process would be agreement on a global instrument providing the required **legal criminal justice instrument for fighting cybercrime** and for facilitating international cooperation between states, based on a clearly defined scope with appropriate safeguards and provisions for technical assistance.
- In addition to the human rights concerns, if the convention departs from existing approaches in defining cybercrime offences, **there is a risk of greater polarisation** among states and to undermining current approaches to Internet governance.
- In addition, if the convention adopts a very different approach in its scope, terminology, and safeguards to existing instruments, it risks creating contradiction with existing national legislation efforts that states have enacted based on existing instruments such as the Budapest Convention.
- Participants agreed that there must be **sufficient expertise amongst the delegations** tasked with negotiating the convention, in particular experts with backgrounds and expertise in law enforcement and criminal justice. This can help ensure that the output from the process accurately addresses the challenges of fighting cybercrime and build on the rich expertise that the diverse range of stakeholders can bring to these discussions.
- It is essential that the new convention builds on past experience, rather than starting from scratch. The experiences that state parties to the Budapest Convention for example can bring to the table are important in developing an operational global instrument to fighting cybercrime that is fit for purpose. The negotiations should take into consideration the **relevant progress and agreements taking place in other international discussions** on the use of ICTs, for example, in the context of international peace and security.
- **Capacity-building** is an essential part of the future convention. Capacity-building helps to address the existing asymmetry between states whether in their understanding of cybercrime or in their capabilities to fight it. However, capacity-building measures must respect the expertise and autonomy of recipient stakeholders.

About Chatham House's efforts to strengthen inclusive and effective cybercrime policymaking

Chatham House is engaging in a multi-year project to strengthen effective and inclusive cybercrime policies, especially at the UN level funded by Global Affairs Canada. As part of this project, Chatham House is offering online training programmes on inclusive cybercrime policymaking, supporting knowledge-sharing on cybercrime issues through the *Journal of Cyber Policy*, implementing a series of Track 1.5 dialogues, and convening regional consultations for non-state stakeholders.

To learn more about Chatham House's work to support inclusive and effective cybercrime policymaking, and for any questions or queries about the summary notes, please contact **Isabella Wilkinson**, Research Associate, International Security Programme, Chatham House, iwilkinson@chathamhouse.org.

About EU Cyber Direct – EU Cyber Diplomacy Initiative

EU Cyber Direct – EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen rules-based order in cyberspace and build cyber resilient societies. To that aim, we conduct research, support capacity building in partner countries, and promote multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in the discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.

To learn more, please visit the project website www.eucyberdirect.eu or contact **Nils Berglund**, Outreach and Public Engagement Coordinator, nils.berglund@iss.europa.eu.