International Security Programme
Consultation Summary

Towards inclusive cybercrime policymaking:

Consultation with non-governmental stakeholders from the Americas region

Event date: 27 April 2022

Independent thinking since 1920

Chatham House does not express opinions of its own. The views expressed in this document are the sole responsibility of the speaker(s)/ participants. Where this document refers to or reports statements made by the speaker(s)/participants at an event, every effort has been made to provide a fair representation of their views and opinions. The published text of a speech may differ from delivery.

10 St James's Square, London SW1Y 4LE T +44 (0)20 7957 5700
contact@chathamhouse.org www.chathamhouse.org
Charity Registration Number: 208223

IGARAPÉ INSTITUTE
a think and do tank

CHATHAM HOUSE

Introduction

Countries across the Americas have suffered a growing wave of cybercrime. The region hosts multiple threat ecosystems where criminal activity has surged at the same time as the digital landscape in the Americas has evolved: these threats range from the use of cryptocurrencies by organized crime groups for the purposes of money laundering, to online fraud, drug-trafficking and the dissemination of child sexual abuse material.[1] Criminal groups and actors in Brazil, for example, have used information and communication technologies (ICTs) to expand their activities, and have targeted countries in North America and Europe.[2] There has also been a reported increase in cooperation between criminal groups within the Americas and, in particular, across Brazil, Peru and Mexico.[3]

In response, countries in the region have developed national regulations to deal with the rise in online organized crime. As part of their efforts to counter cybercrime, 10 countries in the Americas have ratified the Budapest Convention on Cybercrime, with five additional countries in the region having either signed or been invited to accede to it.[4] Governments have also established dedicated units (in the form of either agencies or police units) to combat cybercrime; strengthened regional collaboration between law enforcement actors; and engaged in international efforts on capacity-building and technical cooperation with bodies such as Interpol. However, some of the regulations that have been proposed or enacted to deal with cybercrime have also had adverse impacts on human rights. In addition, while international instruments such as the Second Additional Protocol of the Budapest Convention might have been regarded with greater approval by European countries, ongoing debates in the Americas have shown that the speedy approval of the Additional Protocol could increase law enforcement powers while leaving human rights protections optional.[5] Hence, it is imperative to contextualize and map the potential effects of international instruments across different regions and, in particular, the Americas.

It is against this dense legal and threat landscape that UN member states, including from the Americas, will negotiate a new convention on cybercrime

[1] Muggah, R. (2015), 'The rising threat of organised crime on social media', World Economic Forum, 27 July 2015, https://www.weforum.org/agenda/2015/07/social-media-violence/.

[2] Muggah, R. (2015), 'Gangsta's Paradise: How Brazil's Criminals (and Police) Use Social Media, *Americas Quarterly*, 20 August 2015, https://www.americasquarterly.org/article/gangstas-paradise-how-brazils-criminals-and-police-use-social-media/.

[3] García Caparrós, J. C. (2021), 'Top Cyber Threats to Latin America and the Caribbean', Mandiant, https://www.mandiant.com/resources/top-cyber-threats-to-latin-america-and-the-caribbean.

[4] Argentina, Canada, Chile, Colombia, Costa Rica, the Dominican Republic, Panama, Paraguay, Peru and the US are parties to the convention, while Brazil, Ecuador, Guatemala, Mexico, and Trinidad and Tobago are observers which have been invited to accede. Council of Europe (2022), 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY', https://www.coe.int/en/web/cybercrime/parties-observers.

[5] Gullo, K. and Alimonti, V. (2022), 'EFF, AI Sur Launch Guide to Raise Awareness About Deficiencies in Cross-Border Surveillance Treaty and Strategies to Mitigate Human Rights Risks', Electronic Frontier Foundation, 16 May 2022, https://www.eff.org/deeplinks/2022/05/eff-al-sur-launch-guide-raise-awareness-about-deficiencies-cross-border; Martins dos Santos, B. (2022), 'Budapest Convention on Cybercrime in Latin America', 16 May 2022, DerechosDigitales, https://www.derechosdigitales.org/18451/convenio-de-budapest-sobre-la-ciberdelincuencia-en-america-latina/.

in 2022–23. This will take place in the Ad Hoc Committee (AHC)[6] to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, as mandated by UN General Assembly resolution 74/247 of August 2020. The future convention will determine the parameters of criminal acts in cyberspace. It could help facilitate international cooperation to counter cybercrime and provide technical assistance, and indeed can achieve even more, if UN member states can agree to a new cybercrime treaty at the end of the process. Implementing such a convention could have global consequences, both positive and negative, for fighting the criminal use of ICTs and protecting human rights, both on- and offline.[7]

Delegations from the Americas have been very active in the negotiations to date, from leading on resolutions regarding the modalities of the process[8] to providing written and oral submissions during the sessions. The extent of their involvement highlights the significance that is placed by regional governments on the outcome of the AHC process.

Against this background, on 27 April 2022 Chatham House's International Security Programme and the Igarapé Institute's Digital Security Program convened a virtual consultation for over 30 non-state stakeholders from across the Americas region, representing organizations involved or interested in the AHC process towards a new cybercrime treaty. This session took place under the Chatham House Rule,[9] the organizers having invited participants to share knowledge, information and perspectives on items for discussion at the AHC's second negotiating session[10] (30 May–11 June 2022).

[6] United Nations Office on Drugs and Crime (undated), 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

[7] Brown, D. (2021), 'Proposed UN Cybercrime Treaty Could Undermine Human Rights', Human Rights Watch, 18 January 2021, https://www.hrw.org/news/2021/01/19/proposed-un-cybercrime-treaty-could-undermine-human-rights.

[8] United Nations General Assembly (2021), 'General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations', press release, 26 May 2021, https://www.un.org/press/en/2021/ga12328.doc.htm.

[9] When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

[10] United Nations Office on Drugs and Crime (2022), 'Second session of the Ad Hoc Committee: Vienna, 30 May to 10 June 2022', https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

The consultation provided a platform for discussing the following:

- General provisions [of a comprehensive international convention] and provisions on criminalization; and

- Law enforcement and procedural measures.

This summary document is the outcome both of the discussions held during the consultation and of the written inputs provided by participants after the session. The objective of presenting the main findings in summary form is to provide insights for delegations involved in the AHC ahead of the second substantive session. The summary report can also provide context as well as supporting the work of policymakers and diplomats working nationally and regionally on cybercrime-related agendas.

General provisions and provisions on criminalization

Guiding question*: Reflecting on your work, expertise and/or regional perspective, what should be included in a UN convention on cybercrime? What crimes does the convention need to address?*

- **Precision is imperative with respect to provisions on criminalization.** Participants agreed that provisions on criminalization that are poorly defined in legal terms will raise alarms, because they will be challenging to implement and because they create scope for potential abuses of human rights. For example, in certain countries in Latin America, digital security researchers face persecution for their activities;[11] a new cybercrime convention with ill-defined provisions on illegal access (for instance) could increase the risks and liabilities faced by these researchers.

  Provisions on criminalization should be drafted using technology-neutral language, to 'future-proof' the convention against new technological developments that could be abused by criminals. For example, if the convention criminalizes malicious cyber activities against critical national infrastructure, provisions must be both precise (regarding the types of activities) but also technology-neutral (regarding the types of ICTs that are used or targeted).

[11] Rodriguez, K. (2018), 'From Canada to Argentina, Security Researchers Have Rights–Our New Report', Electronic Frontier Foundation, 16 October 2018, https://www.eff.org/pt-br/deeplinks/2018/10/canada-chile-security-researchers-have-rights-our-new-report.

— **National and regional specificities must be considered when evaluating the effects of cyber-dependent and cyber-enabled crimes.** Participants agreed that cyber-dependent crimes should be addressed by the convention. However, as with many of the points raised by government representatives, there is no consensus as to whether – and which – cyber-enabled crimes should be included. Most participants noted that the convention should adopt a narrow approach to criminalizing activities that extrapolate cyber-dependent crimes. It would not only provide more legal certainty to the text, but would also avoid an excessive juxtaposition of legal regimes.

Across the Americas region, there is a significant amount of regional diversity in terms of different nations' technical, legislative and policy capacity to address the criminal use of ICTs. This inevitably influences each country's choice of priority 'cyber-enabled crimes' to be included in a future convention. Countries' suggestions are also governed by their respective national and regional threat landscapes and pre-existing capabilities. Colombia, for instance, would define the scope of cyber-enabled crimes as extending to drug-trafficking.

— **Strong and clear human rights considerations must cut across provisions on criminalization, or risk creating scope for abuse.** Currently, both in the region and globally, multiple stakeholders (especially civil society organizations) have advocated strongly for the inclusion of human rights safeguards across a list of core (cyber-dependent) offences and a limited number of cyber-enabled offences.[12]

However, many participants raised concerns regarding the risks associated with expanding the scope of the cyber-enabled crimes to be included in the provisions on criminalization. Two main risks were identified and discussed. First, the risk of contradiction and duplication with existing legislation and instruments. Second, the risk of human rights abuse, particularly with regards to content-based crimes. As evidenced by several human rights organizations, many countries around the world have used cybercrime laws to criminalize online content (and freedom of speech) using different pretexts, such as misinformation or 'fake news' offences.

Some stakeholders claimed that even if some cyber-enabled crimes were excluded, this would not mean that they would remain unaddressed. Governments should only include the crimes that are likely to have transnational effects – if, that is, the crimes themselves are considerably amplified and transformed in their speed, scale and scope due to the use of ICTs.[13]

[12] See non-governmental organizations' submissions to the AHC Second Session: United Nations Office on Drugs and Crime (2022), 'Second session of the Ad Hoc Committee'.

[13] Preferences around what provisions, crimes and procedural measures to include in the convention may also be shaped by differences in national capacity to combat cybercrime. During the consultation, participants drew attention to the fact that some small, developing countries in the Caribbean faced capacity gaps.

Participants commented that many national legal frameworks are not strong enough to protect human rights amid the application of a new cybercrime treaty. As such, human rights considerations pertaining to privacy, data protection, etc. (part of a wider set of principles, under the umbrella of the Universal Declaration on Human Rights and other instruments) need to be featured prominently across the chapters and text of the treaty.

Law enforcement and procedural measures

Guiding question*: What are you most concerned with in relation to the procedural measures and law enforcement powers that this convention will provide? What is the approach that the convention should take in order to address these concerns effectively (e.g. human rights protections, stakeholder responsibilities, capacity-building and technical assistance, etc.)?*

— **Access to data should be specific in order to avoid overreach and conflict between laws.** Participants noted that while the convention has the potential to strengthen cross-border collaboration in fighting cybercrime, it is of paramount importance that clear limitations are set as to what it should incorporate in terms of access to data. This includes disallowing the bulk collection of data, ensuring that the convention sets out robust procedural and human rights safeguards, and ensuring that requests are narrow in scope, attending to the principles of necessity and proportionality.

What is more, an overreaching convention would present challenges for future legal harmonization. Conflict between laws deriving from the text could disproportionately affect developing countries. As a result, these nations could face even greater challenges in implementing the provisions of the convention. To take one example, if data retention provisions for internet service providers (ISPs) neither draw on existing legislation nor reflect a narrow approach, they could potentially conflict with national laws, enhancing accountability gaps for access to data by law enforcement agencies, and expanding the challenge for medium and smaller ISPs which might not be adequately prepared to comply with the relevant laws.

— **Capacity-building is a precondition for a forward-looking and rights-respecting convention.** During the first round of the AHC negotiations, most states in the Americas region stressed the importance of capacity-building as a stepping stone for enhancing international cooperation and providing technical assistance. Some participants stated that the convention should ensure that developing countries receive training, and can access knowledge exchange, to help them tackle crimes linked to ICTs. Other countries, such as the member states of CARICOM (the Caribbean Community), supported a proposal for a dedicated fund to support developing countries.

Participants stressed that capacity-building efforts should involve policymakers, incident responders, security researchers and law enforcement agencies, among other communities. In terms of scope, these efforts should concentrate not only on the exchange of techniques and best practices in narrowly focusing on combating cybercrime, but they should help to mature the conversation around specific mechanisms and procedural measures. Participants highlighted how some countries in the region have faced challenges with respect to the formatting of requests for data access: these requests should be clear, and narrow in scope. In addition, a rights-respecting convention would also seek to be human-centric: i.e. it would place the individual at the centre of discussions about prevention and protection. In practice, this would, for example, extend to notifying individuals when their government seeks to access their data.

— **Data access should not be regarded as a 'silver bullet' that will respond to all types of cybercrime.** Participants emphasized that the convention should not be conceived as an all-encompassing solution to existing problems, especially when it comes to facilitating data access. It should support existing best practices, and reaffirm state commitments to enforcing and adopting robust privacy-enhancing legislation. While most discussion around data preservation and access has focused on transnational data as a 'gold standard', improved access to data does not necessarily translate into more effective measures to combat cybercrime.

Participants noted that countries in the region could also profit from revisiting their own national procedures, and reflecting on whether appropriate steps and capacities are in place (with the necessary safeguards) to request data nationally, across sectors and among government bodies. Even though states in the Americas are discussing the potential of the convention to strengthen international cooperation in fighting cybercrime, tackling the lack of coordination and transparency in criminal investigations at the national level should be seen as a precursor for considering the potential effectiveness of an international convention. A lack of understanding among policymakers on how to implement national laws can lead to disproportionately restrictive practices such as IP address blocking, the taking down of services across entire social media platforms, and internet shutdowns, among others. In some instances, these restrictive practices can indeed be deliberate on the part of governments with a more autocratic approach to the internet and cyberspace.

Stakeholders also noted that in the context of big tech companies and social media platforms, it is understandable that there are concerns around crimes and wrongdoing within and among the user base. Even so, many participants stressed that private actors such as ISPs should not be considered agents of public security and law enforcement. The international convention could help ensure that public–private sector collaboration has clear procedures, strong human rights safeguards and independent oversight.

Note: The region of the Americas encompasses multiple types of regional specificities and identities. In organizing the consultation, the project team took into consideration the significance of maintaining regional diversity, in addition to sectoral and gender diversity. To maximize participant engagement, the session was hosted in Portuguese, Spanish and English.

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

This consultation constitutes part of a series that Chatham House is conducting around the world to ensure that there is a platform for multi-stakeholder initiatives in cybercrime policymaking and a channel to include the perspectives of stakeholders in this process. These structures are crucial, given the rich expertise that non-governmental stakeholders from the Americas – and other regions – have brought to their work on a number of issues (including cybercrime, data protection and cybersecurity) at both national and international levels. In fact, non-state stakeholders have invaluable experiences to share in terms of improving the effectiveness and inclusiveness of cybercrime policymaking. In the case of non-governmental actors who might not be actively engaging in or following the AHC, their expertise and insights are crucial in that they reflect specific challenges to the future convention's negotiation and implementation. Their concerns and recommendations should therefore be shared as a matter of priority, given the impact that a future UN cybercrime treaty will have on diverse stakeholders around the world. Chatham House is engaged in a multi-year project with various activities aiming to strengthen effective and inclusive cybercrime policymaking, with the support of Global Affairs Canada.[14]

About Igarapé Institute's Digital Security Program

Igarapé Institute is an independent think-and-do-tank which is devoted to integrating the security, justice and development agendas. The Institute's goal is to propose evidence-based solutions to complex social challenges by producing research, designing new technologies, and shaping public policy. Its Digital Security Program is dedicated to developing interdisciplinary research, fostering multi-stakeholder dialogues and promoting confidence-building to advance agile digital and cyber policies both in the Global South and internationally. This includes building bridges between multilateral agendas and national realities. Igarapé Institute thinks critically about the intersection between the social and technical impacts of emerging technologies, and develops strategies to promote digital rights and algorithmic transparency.[15]

[14] See Royal Institute of International Affairs, International Security Programme (2022), 'Towards an Active Civil Society in Global Cybercrime Efforts', https://www.chathamhouse.org/about-us/our-departments/international-security-programme/towards-active-civil-society-global.
[15] To learn more about the Digital Security Program, please email contato@igarape.org.br, or to access the Brazilian Cybersecurity Portal directly, please visit https://ciberseguranca.igarape.org.br/. See also Igarapé Institute (undated), 'Digital Security', https://igarape.org.br/en/digital-security/.