Global Cyber Policy Dialogues: Latin America & the Caribbean

December 13-14, 2022
Santiago, Chile

MEETING SUMMARY

Ministerio de Relaciones Exteriores
Gobierno de Chile

Ministry of Foreign Affairs of the Netherlands

ORF AMERICA

UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO

On December 13-14, 2022, the Ministry of Foreign Affairs of Chile and the Ministry of Foreign Affairs of the Netherlands, in partnership with Observer Research Foundation America and the Centre for Information Technology Law Studies (CEDI) hosted an in-person Global Cyber Policy Dialogues: Latin America and the Caribbean meeting in Santiago, Chile. The meeting brought together 45 participants from across the Latin American and Caribbean region, representing government, civil society, academia, multilateral institutions, and the private sector. The discussion considered the United Nations (UN) normative framework for cyber stability, international cooperation to combat cybercrime, the intersection between those two areas and UN processes, and how digital transformation in Latin America can be enabled by an open, free, stable, and secure cyberspace.

A virtual preparatory meeting was held in January 2022 to lay the groundwork for this event, and a summary is available to provide further background. The virtual meeting addressed the normative framework for cyberspace, digital transformation enabled by cyber stability, and the threat of cybercrime in the region. In particular, the discussion produced insights about the foundational role of capacity building to international cooperation on information and communications technology (ICT) matters, the relationship of human rights to cybersecurity and cybercrime policies, the need for practical cooperation to address cybercrime, and the opportunities for trust-building presented by the international processes on ICTs.

The two-day meeting began with a reception hosted by the Dutch Ambassador where the delegates connected and shared perspectives and viewpoints on an informal basis. The following day consisted of four working sessions, conducted in roundtable format so as to maximize participation and diversity of viewpoints. This dialogue was convened as part of the Global Cyber Policy Dialogue Series, a project undertaken by ORF America and the Ministry of Foreign Affairs of the Netherlands. This project consists of regional meetings which seek to address key cyber challenges, strengthen multistakeholder networks, and increase coordination of regional capacity-building initiatives. These meetings are intended to complement ongoing international-level cyber processes, such as the United Nations Open-ended Working Group and Ad Hoc Committee on Cybercrime.

The discussions took place under the Chatham House Rule. Opening remarks for the meeting were provided by Felipe Cousiño, Head, International and Human Security Division, Ministry of Foreign Affairs of Chile, Maartje Peters, Head, Taskforce International Cyber Policy, the Ministry of Foreign Affairs of the Netherlands, Daniel Álvarez Valenzuela, National Cybersecurity Coordinator, Ministry of the Interior and Public Security of Chile, Director, Centre for Information Technology Law Studies (CEDI). The meeting was moderated by Bruce W. McConnell, distinguished fellow at ORF America.

The United Nations Normative Framework for Cyber Stability

The first session on December 14 focused on the recent meetings of the United Nations Open-ended Working Group (UN OEWG), efforts that Latin American stakeholders have been undertaking to implement agreed outcomes, as well as prospects for future agreement on the international level.

The session began with remarks by G. Isaac Morales Tenorio (Ministry of Foreign Affairs of Mexico), Pablo A. Castro (Ministry of Foreign Affairs of Chile), Kerry-Ann Barrett (Organization of American States (OAS), and recorded remarks from Marilia Maciel (DiploFoundation). During the discussion, participants reaffirmed that a free, secure, and resilient cyberspace is not possible without multilateral cooperation and the engagement of all stakeholders. Some attendees called attention to the fact that it had been difficult for non-state stakeholders to meaningfully participate in the OEWG process. They called for all present to take action to ensure that any future Programme of Action or future process includes meaningful participation by all, which will be necessary to really implement the normative framework. Examples of other initiatives, such as the Geneva Dialogue, were given to demonstrate how other stakeholders, particularly companies, can participate. Similarly, it was noted that the UN is not the only forum to have discussions about norms

and responsible behavior in cyberspace. Regional organizations, NGOs, and multistakeholder forums are all active in this space and carrying out implementation activities. Participants particularly noted the role that academia can play in providing research and recording of efforts and obstacles encountered.

The role of regional organizations as implementers was also discussed, and some voiced that more space should be given in international discussions for regional and sub-regional needs. Regional organizations can be good vehicles for dialogue at a minimum, and some, like the OAS, have been deeply involved in promoting cooperation in cyberspace for many years. They have experience and lessons from capacity-building approaches and confidence-building measures among diverse membership that can be useful to international and other regional conversations.

While reflecting on the status of the UN negotiations in the OEWG, participants noted positive trends, such as the fact that cyber stability has become a foreign policy issue and is being mainstreamed within governments. At the same time, it was clear that many see a challenging road ahead. The current geopolitical situation makes diplomacy difficult, and some assessed that much of the low-hanging fruit has been picked and further consensus will be difficult to achieve on the remaining, more complex issues like international law. Nevertheless, attendees felt it was important to continue to try and find concrete solutions to the complex problems in cyberspace, and the proposed points of contact network that is being negotiated was given as an example of such a solution.

On some of the more difficult topics, it was mentioned that while many characterize cyberspace as "borderless" it is clearly territorialized in some sense, because there is infrastructure that exists physically in specific territories, and this will impact different aspects of the discussions. For example, it was noted that while conversations about human rights should be universally applied, aspects related to infrastructure will concern national jurisdictions. The question of due diligence also came up, in terms of states' responsibility to respond to requests for information on threats emanating from their territory and to take action. While information sharing sometimes happens more easily on the technical level, it was clear there is some work to do in responding to requests at higher political levels, and in international discussions questions of due diligence raise issues of international law, which can quickly become complex. Participants reaffirmed the need for countries in the region to publish their views on how international law applies in cyberspace, in line with the OEWG recommendations.

International Cooperation to Counter Cybercrime

The second session shifted focus, looking at cyber attacks carried out by criminals for financial gain, some of which may be sponsored or condoned by the governments of the countries where the attackers reside. States face difficult challenges combating criminality in the digital space. The virtual meeting highlighted the need for practical avenues for cooperation across borders to effectively counter cyber criminals, and this session provided an opportunity to discuss efforts within states as well as the negotiations to create an international treaty on cybercrime.

The session began with remarks by Claudio Peguero Castillo (UN Ad Hoc Committee on Cybercrime), Grecia Elizabeth Macías Llanas (Red en Defensa de los Derechos Digitales (R3D)), Andrés Camilo Ramírez Espitia (National Police of Colombia (C4)), and Daniela Schnidrig (Global Partners Digital). The discussion focused on the current status of cybercrime negotiations in the UN Ad Hoc Committee, noting that from the outset the goal of creating an international cybercrime treaty was ambitious. All states had different things they wanted from a treaty. There are different options for the scope of the treaty, and different views on what it should be. Participants involved in the negotiations stated that in January 2023, when conversations start on the wording, it will get more difficult. The view was expressed that ultimately, any treaty will be a criminal justice instrument, and if this process can generate certainties and safeguards to ensure that requests for evidence will be subject to judicial review, it would be a useful contribution. Another positive

development shared from the Ad Hoc Committee process was that some states, upon hearing more about the Budapest Convention during the discussions, had joined the Convention.

Some participants from civil society expressed concern about the scope of the treaty and called for thinking critically about whether a treaty is even necessary. They drew parallels with other cybercrime laws developing in certain countries. The example was given of discussions in Mexico where they are considering creating a crime of "electronic extortion," which is seen as unnecessary as extortion of any type is already illegal. Moreover, some parties cautioned against overly broad cybercrime laws that over-criminalize and can have negative impacts on freedom of expression and privacy. All cybercrime laws (and a potential treaty) need to respect the principles of proportionality, legality, and necessity.

It was stressed that governments should develop cybercrime laws in processes that are transparent, with opportunity for civil society input. This sparked a discussion about how civil society can demonstrate its value-add for such discussions. Highlighting case studies of where civil society added value and taking the time to build trust within communities were mentioned as key to engaging with states and getting them to respond to and include civil society. A few case studies were highlighted in the discussion, including the role that NGOs played in developing Chile's national cyber policy, where input was brought in from a much broader network.

Some government representatives focused on the complexity of cybercrime, and the challenges they face in adequately addressing it. Lack of capacity, including human resources, was brought up, as often the private sector can pay more than government.

Intersection between Cyber Stability and Cybercrime

The third session focused on the intersections that exist between efforts to ensure cyber stability and to combat cybercrime, in particular between the processes in the UN General Assembly's First Committee (OEWG) and Third Committee (Ad Hoc Committee on Cybercrime). While there are reasons to keep the two processes distinct in the context of the UN, the massive ransomware attack against Costa Rica provided a regional illustration of how cybercrime can present a threat to the stability and security of an entire country. This session invited participants to explore the connections between the two topics, as well as the two UN processes.

The session began with remarks by Ana María Pinilla Morón (Ministry of Foreign Affairs of Colombia), Nicolás Vidal (Ministry of Foreign Affairs, International Trade and Worship of Argentina), Mariel Aranda (Paraguay Chapter, Internet Society), and a recorded video from Paula Brenes Ramírez (Ministry of Science, Innovation, Technology and Telecommunications of Costa Rica). The discussion focused heavily on the potential connections between the UN processes. There was some disagreement about whether or not there needed to be a strict "wall" between both processes. It was acknowledged that the OEWG and cyber stability discussions are more political considerations. Many want the cybercrime negotiations to stay more pragmatic. However, others pointed out that there are instances where cybercrime has political dimensions: e.g., the ransomware attack in Costa Rica, or other attacks on critical infrastructure. Participants also noted that there are also several norms from the First Committee processes, the OEWG and Group of Governmental Experts (UN GGE), that are relevant to combating cybercrime: states should cooperate to hold cyber criminals accountable, not allowing use of their own infrastructure to conduct attacks, and that states should cooperate in response to attacks on critical infrastructure.

Proposals for recognizing the distinction between the groups while enabling coordination were discussed, in order to increase mutual awareness. One idea was having the chairs of both groups co-convene an informal, intersessional meeting to report on the status of negotiations. This would not mix agendas or participation across the groups, but merely create space to maintain awareness among representatives and non-state stakeholders in both groups and to think strategically about future engagement. Other

participants advocated that a key outcome for both processes is shared terminology and definitions of key terms. There was an interest in understanding who is keeping track of agreed language or definitions. It was also conveyed that human rights are a shared topic across both processes.

Despite legitimate reasons to keep the negotiations separate in the UN context, in practice, links between cyber stability and cybercrime are evident. Attendees emphasized the difficulty in creating an open, stable, and secure cyberspace when there are rampant ransomware attacks on critical infrastructure. Responses to such attacks involve a huge community, including Computer Security Incident Response Teams (CSIRTs), defense agencies, and civil infrastructure. Several parties shared how their governments are approaching these issues, including some which are considering combining cybersecurity and cybercrime under a single agency, and utilizing the concept of "digital security" which covers a broad range of issues. Insights were shared from Colombia's new plan to create such a single cyber agency. Their hope is that with everyone together in one agency, response times can be shorter and more efficient in the face of cyber attacks and agencies can draw on each other's expertise. It was acknowledged that the best appropriate institutional arrangement for each country will be unique.

Digital Transformation Enabled by an Open, Free, Stable and Secure Cyberspace

The final session of the day focused on connections between security and digital development. The UN development goals and digital transformation strategies are all underpinned by strong cybersecurity. Implementing the UN normative framework and combating cybercrime are key pieces that can contribute to digital transformation at the domestic and regional level. There are also capacities, such as incident response and critical infrastructure protection, that support both digital transformation and cybersecurity.

The session began with remarks from Chris Painter (Global Forum on Cyber Expertise), Cristian Eduardo Lira Fuentes (Secretary of Innovation of the Presidency of El Salvador), Agneris Sampieri (Access Now), and Daniel Álvarez Valenzuela (Ministry of the Interior and Public Security of Chile). The discussion highlighted the need for interaction and coordination between economic agencies and cyber agencies. While many countries think that digital economies will grow their economy, there is not a lot of interaction between economic agencies and cybersecurity agencies. They fail to realize if they want to reach this higher level of digitization but do not have good cybersecurity, the effort can falter and digital transformation will not result in the desired level of innovation and growth. Participants agreed that a key element going forward is to involve more economic ministries in these kinds of conversations, and to encourage the cybersecurity communities to participate in development and economic forums to enhance the coordination, even informally.

One challenge raised was capacity. Participants noted that governments need to address cybersecurity intentionally and implement a strategy to improve the underlying infrastructure, but there are limited resources. One participant shared a model their government is developing that includes protection, detection, and trying to identify critical services to prioritize. While they would like to do everything at once, it must be done in stages as there are limited resources. In addition to technical infrastructure, others also spoke of the imperative for legislative and judicial infrastructure to be in place. Laws are needed to hold cyber criminals accountable and there should be technical regulations and cybersecurity standards, as well as national cyber strategies. This discussion also touched again on the question of institutional design, and whether having a single cyber agency to coordinate all matters, including digital transformation, could be useful. This also turned to the topic of CSIRTs, and attendees discussed where CSIRTs sit within government, stressing that a CSIRT can be anywhere so long as they have the necessary authority and are properly empowered and given necessary resources. They need to have that authority and backup to execute their mandate.

Civil society representatives again emphasized the need to involve all stakeholders in digital transformation strategies and discussions. Without multistakeholder involvement, certain aspects could be overlooked in

the development of initiatives, and certain harms could be caused. An example was given in the case of Mexico, where the government undertook efforts to reduce the digital divide by supplying new antennas to provide internet service. However, the agency designated to be in charge of the infrastructure is the military, which can have some implications on trust.

Participants also noted the importance of addressing the issue of trust in digital transformation initiatives. Governments have a responsibility to be transparent with citizens about how technology is being used and governed, to protect human rights, and to ensure the security of information. It is not always a given that citizens trust what governments are doing with digital tools, and certain relationships and arrangements need to be questioned.

Concluding Remarks

Concluding remarks at the end of the conference provided an overview of themes from the dialogue, including the prospects for further international agreement and cooperation on the UN normative framework, the goals of the international process to negotiate a cybercrime treaty and challenges countries in the region face to counter cybercrime, how to improve coordination between the two UN processes, and the need to better connect digital transformation with cybersecurity. The discussions identified several areas for potential future research or projects which are outlined below.

The United Nations Normative Framework for Cyber Stability

- **Ensure multistakeholder participation in future mechanisms:** As the Programme of Action is currently being discussed and details negotiated, all actors, especially states, need to be active to ensure mechanisms for multistakeholder engagement. Future engagements could focus on building a consensus of like-minded states and pushing for concrete language and mechanisms for non-state participation.
- **Amplify and utilize lessons learned from regional organizations:** Several regional organizations are active in implementing different elements of the normative framework and have been even before the current OEWG. While the OEWG has often called attention to the relevance of regional organizations in its reports, more systematic efforts could be undertaken to compile, amplify, and apply lessons and good practices from the experience of regional organizations – both on international and subregional levels.
- **Dig into tough topics, or concrete actions:** If much of the low-hanging fruit has been picked in terms of reaching consensus on the OEWG's agenda, then any future agreements will take time and effort to achieve. Future engagements could focus on a specific aspect – due diligence, for example – and start convening conversations on a regional or subregional basis, with the aim of building foundational trust and understanding. Similarly, such conversations could also be convened to further some of the concrete actions proposed already, for example the points of contact network.

International Cooperation to Counter Cybercrime

- **Make the case for multistakeholder engagement**: The discussion raised the need for civil society to demonstrate their value-add to cybercrime legislative processes. A future initiative could help compile case studies of civil society's engagement and outline the benefits of their involvement, as well as best practices for transparent and inclusive processes. This could be shared throughout the region to expand engagement.
- **Create a framework for building safeguards**: Overly broad cybercrime laws can have negative impacts on human rights or enable abuse by governments. Analyzing a few of these cases, as well as examples of cybercrime laws that are effective and rights-respecting, could be useful to create a framework for understanding how to construct laws to effectively counter this threat while also ensuring human rights are upheld. Meetings could be convened to engage law enforcement, judiciaries, and legislators to better understand the nuance of these conversations.

Intersection between Cyber Stability and Cybercrime

- **Convene an intersessional meeting for the Ad Hoc Committee and OEWG to report on recent discussions**: this could be done by the chairs of each committee, or less formally by a regional organization or another stakeholder. The critical thing is to allow an opportunity for representatives and stakeholders to hear updates about each group.
- **Examine different institutional arrangements to enhance coordination and efficient response to cyber threats**: While some countries may want to pursue a single-agency arrangement, there are other arrangements and practices that can facilitate coordination and information-sharing among agencies. Conversations could be convened to explore different options in this regard and learn from the experience of others.

Digital Transformation Enabled by an Open, Free, Stable and Secure Cyberspace

- **Engage economic and development ministries, agencies, and stakeholders in cybersecurity forums, and vice versa**: In the discussion, it was clear there is a need for greater engagement between the two communities. This can start with more presence – roundtables and conferences could be convened on aspects of digital transformation that bring the two communities together.
- **Improve transparency in digital transformation development and governance**: When governments are undertaking digital transformation initiatives, or developing overarching strategies, they should take a transparent approach that seeks input from other stakeholders. Examining best practices in this regard could offer guidance on how to achieve more meaningful civil society participation and input, as well as transparency.