GLOBAL CYBER POLICY DIALOGUES: LATIN AMERICA

January 13, 2022
11:00-12:30 CLST

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

Meeting Summary

On January 13 the Ministry of Foreign Affairs of Chile and the Ministry of Foreign Affairs of the Netherlands, in partnership with Observer Research Foundation America (ORF America) and the Centre for Information Technology Law Studies (CEDI) hosted a virtual *Global Cyber Policy Dialogues: Latin America* meeting. The meeting focused on the linkages between the cyber stability normative framework, international cooperation to counter cyber crime, and the importance of an open, free, stable, and secure cyberspace to enabling digital transformation in the region.

This event is part of a larger Global Cyber Dialogue Series being undertaken by ORF America and the Ministry of Foreign Affairs of the Netherlands, which seeks to convene regional meetings 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 at the United Nations and other forums, and this meeting in particular was designed with a specific focus on cyber crime in order to facilitate an exchange of regional views ahead of the first session of the UN “Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes” (UN Ad Hoc Committee on Cyber Crime).

The meeting kicked off with opening remarks from **Ambassador Gloria Navarrete**, Secretary-General for Foreign Policy of the Ministry of Foreign Affairs of Chile and **Ambassador Nathalie Jaarsma**, Ambassador-at-Large for Security Policy and Cyber of the Ministry of Foreign Affairs of the Netherlands. A panel discussion followed, covering a wide range of topics including the foundational role of cyber capacity building, the need for more practical cooperation on cyber crime, increased clarity in cyber crime legislation and terminology to protect against human rights abuses and enable effective international cooperation, and opportunities to engage in international processes as a way to build trust.

Summary of Key Points from the Discussion

Ambassador Navarrete opened the meeting with a characterization of the situation currently facing governments: malicious cyber activity poses a threat to international security, critical infrastructure, and development gains, and states have a responsibility to work together to reach agreements to secure and stabilize the ICT environment. She highlighted Chile’s efforts in this regard, as Chile was the first country in South America to join the Budapest Convention on Cybercrime and has enacted domestic cyber crime laws reflecting international standards. Turning her focus to the ongoing international processes, she noted the opportunities processes such as the current UN Open-ended Working Group (OEWG) or the UN Ad Hoc Committee on Cyber Crime present for Chile to give input and contribute to building trust in cyberspace. Amb. Navarrete also noted that these efforts should include gender dimensions and involve all stakeholders, not just states. She identified a few areas where additional progress must be made in the Latin America and Caribbean region, including on the design and implementation of national cybersecurity strategies and improving regional cooperation in particular. Noting the role the Organization of American States (OAS) has played in facilitating regional cooperation and trust-building through the establishment of the Working Group on Confidence-Building Measures in Cyberspace, Amb. Navarrete emphasized the importance of such fora for exchanging views and best practices, which leads to greater trust and greater collaboration in this sensitive domain.

Ambassador Jaarsma echoed Amb. Navarrete’s characterization of cyberspace, asserting that it is clear that cyberspace is not automatically a force for good. Careful interventions by all stakeholders are required in order to ensure that existing social and economic inequalities are not replicated or deepened by digital technologies, and that threats are managed responsibly. In this context, Amb. Jaarsma highlighted the importance of efforts to enable young people and women in particular to participate in the digital economy. She also took up the issue of trust, noting two sides of trust that are central to efforts to bridging the digital divide: the technical side and the human side. On the technical side, citizens, companies, and organizations must trust the security of the digital tools they use in everyday life, have confidence that their data is not being stolen or misused, and that the general availability of the Internet will not be disrupted. Any interference with the so-called "public core" of the Internet—the infrastructure that enables the basic connectivity and backbone of the Internet—would undermine this. The human side of trust is the trust between citizens, companies, and governments that enables a stable environment in which all stakeholders can work together to build a flourishing digital economy. In order to ensure both sides of trust, Amb. Jaarsma outlined three principles: inclusivity, responsibility, and sustainability, accompanied by concrete lines of action.

After the opening remarks, a panel of experts tackled the issues around implementing the cyber stability normative framework, improving international cooperation to counter cyber crime, and the importance of an open, free, stable, and secure cyberspace to enabling digital transformation, featuring the following speakers:

- **Kerry-Ann Barrett**, Cyber Security Policy Specialist, Inter-American Committee against Terrorism, Organization of American States
- **Claudio Peguero Castillo**, Vice-Chair, UN Ad Hoc Committee on Cyber Crime
- **Barbara Marchiori de Assis**, Lecturer, International Program on Cybersecurity and Privacy Management, ESAN University
- **Luis Fernando García**, Executive Director, Red en Defensa de los Derechos Digitales (R3D)
- **Daniel Álvarez-Valenzuela**, Professor, Faculty of Law, University of Chile

The panel was moderated by **Bruce W. McConnell**, Distinguished Fellow at the Observer Research Foundation America. The following sections highlight key themes from the discussion.

Capacity building is foundational to international cooperation

Kerry-Ann Barrett began the discussion emphasizing that there are certain capacities that are needed for states to effectively combat cyber crime and ensure cybersecurity. She noted that there is no prescriptive way to build capacity or to combat cyber crime or a "one size fits all" solution. All states have a variety of capacities and needs, and an assessment conducted in 2020 gives an overview of the various stages of maturity throughout the region. The OAS plays a supporting role in capacity building, assisting with creation of incident response plans, legislation, strategies, and partnerships between stakeholders in the region. The Cyber Security Program of the OAS Inter-American Committee Against Terrorism (CICTE) works to operationalize skills needed to address cyber crime and security, including responding to specific capacity requests to establish incident response capabilities. They also run the CSIRT Americas network, which promotes cooperation among incident response teams in the region. The OAS Meetings of Ministers of Justice or Other Ministers of Attorneys General of the Americas (REMJA), houses a cyber crime working group that gives advice to member states about how to investigate and prosecute cyber crime. The OAS is also working with the Global Forum on Cyber Expertise (GFCE) to create a regional capacity building hub for Latin America.

Claudio Peguero also highlighted the need to strengthen capacities of law enforcement and judicial systems to effectively combat and prosecute cyber crime. He noted that best practice exchanges and peer-to-peer learning can be beneficial, for example having legislators meet their peers in other countries who are working on cyber policies and laws. In this regard, Barrett noted that there is a knowledge gap in national legislatures around cyber issues that should be discussed. Capacities are needed at the national level, as well as for legislators to understand how to cooperate internationally on these matters. Peguero concurred, noting that building cyber capacity is a continuous process. He highlighted the experience of the Dominican Republic, which took three years to create cyber crime legislation, a process that included holding workshops with legislators to improve their understanding of the issues. Now a similar process is starting with data protection legislation. Barbara

Marchiori also highlighted capacity gaps that pose challenges for cooperation in the fight against cyber crime, citing specific issues like electronic evidence collection and exchange.

The need for practical cooperation to address cyber crime

Claudio Peguero gave an overview of the current processes at the United Nations addressing stability and security in cyberspace. While the OEWG is a diplomatic process, he noted that the new Ad Hoc Committee on Cyber Crime is focused on creating a criminal justice instrument and thus must be more concerned with practical matters. The goals of the Ad Hoc Committee are to reduce impunity, assist victims, and ensure accountability for cyber crimes, which requires effective cooperation. In response, Bruce McConnell noted the difficulty of achieving cooperation on a practical level especially when each state has its own legal instruments, judicial systems, and laws governing what is considered criminal in cyberspace. He gave an example of freedom of speech law in the United States which allow for some content to be posted online that in other countries may be considered criminal hate speech or incitement. This line of discussion raised the issue of the role of private sector companies, in particular platform companies, as they are often seen as taking on an extra-judicial role by policing activity on their sites based on their own interpretations of their terms and conditions or user agreements.

The challenge of practical cooperation when so much ambiguity exists around states' understandings of what constitutes cyber crime or how each other's legal and judicial systems function was a common thread picked up by many of the speakers. Kerry-Ann Barrett noted at the outset that the OAS believes many terms and definitions used in relation to cyber crime require further clarity and a common terminology is needed in order to do any mutual legal assistance. Barbara Marchiori amplified the point, noting that national definitions of cyber crime vary across the region, and if you were to look at all the definitions together, anything can be considered cyber crime. The lack of specificity is a danger when going into multilateral negotiations like the Ad Hoc Committee. Luis Fernando García underscored this point, citing a letter written to the Chair of the Ad Hoc Committee on Cyber Crime from civil society organizations (English and Spanish versions of this letter are available). He noted concern from civil society about the lack of universal understanding about what a cyber crime is, and that the proliferation of vague and imprecise classifications can lead to creeping definitions and catch-all laws open to abuse. In the cyber context, he gave the example of including "unauthorized access" as a cyber crime, which is a vague term and has led to the criminalization of IT investigators or "white hat hackers" who are identifying vulnerabilities in IT systems. Conversely, Peguero argued that prior authorization should be a requirement and unauthorized intrusions into a company or organization's IT systems should be criminalized. Otherwise, he reasoned, criminals who hack into a company's system can just claim they are helping the company to identify vulnerabilities and the company, who never asked for help, would be left with no recourse. Thus, it is important to have some kind of framework in place to identify who is an authorized security researcher or "white hat hacker" and who is not. Fernando García maintained however that the public interest in having vulnerability research and disclosure, which sometimes may not be in the business interest of a company or government, means that even non-authorized IT investigators should be protected under the law. His position was that laws should not just be based on authorization, but on intent and impact.

Another concrete example of ambiguity obscuring practical cooperation was given by Peguero. He shared that member States of the Budapest Convention are discussing the development of an online tool to give states and private sector service providers information on who is authorized to request information from private companies in different countries. In some countries, the police can issue a subpoena, in others it has to come from a judge or prosecutor to be lawful. Clarity on these points would help states effectively cooperate in a timely manner, ensure that companies are following the correct laws, and that existing rights are upheld.

Relationship between human rights and cybersecurity and cyber crime policies
The concerns about a lack of clarity in legislation and terminology around cyber crime raised by Luis Fernando García and Barbara Marchiori highlighted the need to ensure that human rights and fundamental freedoms are protected as states endeavor to strengthen cybersecurity and combat cyber crime. Fernando García challenged the notion that the issue of cyber crime is a binary issue with the "good guys" (the governmental authorities) on one side and "bad guys" (cyber criminals) on the other. The reality is more complex, he argued, giving the above-mentioned example of white hat hackers being caught up in laws criminalizing unauthorized access, and how broad categories of crimes have been used by governments to target and spy on journalists and political adversaries or activists. He also noted that any international agreement about access to evidence should be conditional on states having robust institutional framework to safeguard privacy and prevent human rights violations.

Daniel Álvarez-Valenzuela also noted that states' obligations to apply international law in cyberspace include obligations to respect human rights. Marchiori brought in the role of the private sector here, highlighting that they also have a duty to protect the human rights of their users through their data protection policies. She noted that data collection and protection is a big issue for the Latin America and Caribbean region currently. With respect to the role of companies, Claudio Peguero also commented that states and service providers need to trust each other to ensure that laws are upheld. When looking at all the requests that states make to companies, the rate of reply varies from state to state, as technology companies trust some states more than others because of how they behave and whether they uphold human rights norms.

International processes on ICTs offer opportunities to build trust
In his closing remarks reflecting on the discussion, Daniel Álvarez-Valenzuela noted that the international processes on ICTs taking place at the UN and elsewhere offer opportunities for states and other stakeholders to engage with each other and build trust around these important and multi-dimensional issues. In this regard, he especially highlighted the OEWG as a more open, transparent, and inclusive process and hopes that states and stakeholders will engage with the ongoing iteration. This echoed the points made by Ambassadors Navarrete and Jaarsma at the outset, calling for more inclusive processes that involve all stakeholders and consider the needs and priorities of different and sometimes marginalized communities.

Álvarez-Valenzuela underscored the importance of transparency on the part of states as they create and apply policies on cybersecurity and cyber crime as an element of improving trust. He noted that in the Latin America and Caribbean region, 14 countries have national cybersecurity strategies and all declare they are consistent with the principles and norms agreed to at the international level through the UN. However, there is little transparency about how these policies actually work in practice to uphold those principles. Álvarez-Valenzuela concluded with the idea that the ultimate goal of improving security in cyberspace is to build open, free, and secure spaces where people can live their lives and use their talents.

Looking Ahead

In an effort to contribute to the move from discussion to action, the following areas from the meeting have been identified for further engagement:

1. **Building avenues for practical cooperation with appropriate safeguards:** International cooperation to combat cyber crime is necessary because of the borderless nature of cyberspace. Yet conflicting cultural or political norms and laws around criminality, the applicability of certain rights, and the role of the private sector introduce ambiguity. The UN Ad Hoc Committee represents the start of a process to craft an international convention to facilitate cooperation to combat cyber crime including through processes for evidence sharing, mutual legal assistance, and capacity building. These avenues of

cooperation should also include safeguards against overreach and function creep, and provide for the protection of human rights. Further efforts could focus on specific cooperative mechanisms (digital evidence sharing, streamlined assistance procedures, for example) and the relevant impacts in areas such as human rights, data protection, and innovation. They could produce recommendations or frameworks for an international agreement to adhere to when facilitating cross-border cooperation.

2. **Harmonizing cyber crime terminology:** As was noted by several speakers throughout the discussion, a significant challenge to effectively cooperating in efforts to combat cyber crime is the lack of common terminology. While states do not need a universal legal definition of cyber crime, agreeing on the meaning of other basic terms can be helpful in communicating and taking joint action in response to malicious ICT acts. Future efforts could identify terms that are necessary to enable mutual legal assistance and cooperation, and develop basic common terminology or compile existing definitions of key terms to further mutual understanding among stakeholders.
3. **Exploration of the role of the private sector:** A common refrain in multilateral discussions about stability in cyberspace and cyber crime is that the private sector has an important role to play. More meaningful conversation with the private sector could be useful in furthering implementation of the international framework for cyber stability, as well as any agreement on cyber crime cooperation. In particular, engagement with small and medium-sized enterprises should be emphasized. As the speakers at this meeting noted, the private sector is currently playing multiple roles including as extra-judicial arbitrators enforcing their terms and conditions and responding to government requests for information, and as first-line defenders against criminals as they operate (sometimes critical) IT infrastructure. Private companies also have a key role to play in digital transformation. A series of engagements that bring together private sector actors from a variety of industries and types of companies could provide opportunity to explore the impacts of proposed national cyber crime legislation or international agreements on private business as well as their role in implementation.
4. **Enhancing national level capacities for international cyber cooperation:** Speakers noted the challenge that legislating on cyber issues poses for lawmakers, who often do not have technical expertise. International cooperation on these issues is an additional challenge. Convening a session to connect national policymakers with their international counterparts and diplomats could help strengthen the understanding of the international dimensions of cybersecurity issues. Engagement with organizations like the OAS and GFCE that are currently leading cyber capacity building initiatives within the region can help avoid duplication of efforts.