Global Security Review

Volume 2 *Strategic Competition: Russian and Chinese Influence in Latin American and the Caribbean*

Article 7

January 2022

Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America

Louise Marie Hurel
Igarapé Institute,

Recommended Citation
Hurel, Louise Marie (2022) "Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America," *Global Security Review*: Vol. 2 , Article 7.
DOI: 10.25148/GSR.2.009786
Available at: https://digitalcommons.fiu.edu/gsr/vol2/iss1/7

Louise Marie Hurel

The past decades have been marked by a renewed interest from states in enhancing their cyber capabilities. Responses to evolving threats have ranged from establishing designated bodies for cybersecurity at the national level, such as cyber commands, to sanctions and cyber diplomacy as part of the ever-expanding national cyber policy 'toolbox'. Countries such as the United States, the United Kingdom, and their allies have increasingly focused on questions related to offense-defense balance as part of designing their deterrence strategies in cyberspace. Concerns around the asymmetrical nature of cyber threats and the lower barriers of entry for non-state actors (although, at times, state-sponsored) have equally contributed to the emergence of concepts such as "active cyber defense," "defend forward," and "persistent engagement" as synonyms to "authorized offensive cyber operations."[1] In so doing, states believe they can shift the incentives and heighten the costs for adversaries (e.g., China, Russia, and North Korea) to engage in malicious activity[2] while also staging a show of force.

While important, discussions around cyber operations and threats have largely concentrated in a handful of countries[3] – aided by structural factors that include but are not restricted to: the concentration of media coverage in specific countries,[4] stakeholder biases in threat reporting[5], the reproduction of donor-recipient/north-south logic through cyber capacity-building programs, among other elements.[6] In addition to these factors, discourses that seek to reinforce a "great power rivalry"[7] – so often mobilized for capturing competition among "cyber powers"– add to the list of dynamics that obfuscate the scope of the study of global cybersecurity politics, in general, and Latin America, in particular.

Cybersecurity is contextual. Threat perceptions, discourses and policies do not exist in a vacuum but co-exist in different cultural, political, social and economic contexts. While it might seem slightly trivial to remark such a point, the great power rivalry discourse and the over-emphasis on a small group of "power-full" countries hinders the understanding of cyber politics as something that can unfold in other spaces/places.

The focus of this paper is not one of tracing the above-mentioned challenges per se (as that would require multiple papers) but one of recentering Latin America as part of the cybersecurity construct while recognizing global constraints to the interpretation and understanding of how countries beyond the great powers conceive of cyber operations.

This paper addresses a much less visible, but perhaps more concerning outcome of designing great/middle power borders: It can often overlook significant reinterpretations of what cyber operations mean domestically as one shifts to different threat landscapes and across varying levels of capacities (and government bodies) to identify, assess, attribute, and respond to attacks.

To address how cyber operations and cyber norms are conceptualized in Latin America, this paper is divided into three parts. The first part looks at how countries across the region have sought to devise specific mechanisms to tackle cybersecurity issues regionally and how some have started to craft more concrete interpretations of cyber operations under international law. The second focuses on how cyber operations are increasingly positioned in a complex association between public security forces and intelligence activities. Finally, the paper concludes with remarks about the consequences and challenges the relationship between public security and cybersecurity poses to countries in the region. In so doing, I hope the paper can challenge the borders of what is conceived as cyber politics, who can shape cybersecurity and shed light on the existing inequalities that permeate the literature and discussions around cyber operations. However, I do not assume aprioristically that there is a clearly defined uniqueness to Latin American countries' approaches to cyber operations and international cyber norms. Rather, I seek to refocus the discussion on both the former and the latter in the exercise of departing from the complex reality of cybersecurity in the region.

Who's great? Great Power blindfold?

The release of President Biden's Interim National Security Strategic Guidance in March 2021 and other reports and interviews with White House spokespersons indicated a new shift in vocabulary from "great power competition" to "strategic competition" for dealing with China and other actors.[8] In practice, the proposal for a new "strategic" narrative from the Biden administration may be discursively less explicit about rivalry, but it is still primarily concentrates in framing the United States engagement with China and Russia while collaborating with P5 and allies. As previously mentioned, while the great powers are not the focus of this paper, I highlight three dynamics that set the scene of contentions for the study of concepts such as cyber operations beyond the "great powers" and thus paving the way for situating Latin American countries in this landscape.

First, the great power construct often incurs in an over-simplification of state-state relations in which private companies have considerable power over the

governance of networked infrastructures and the production of knowledge about threats.[9] The ransomware attacks promoted by the Russian group Darkside against the state-owned Brazilian energy supplier Copel[10] and, most notoriously, Colonial Pipeline,[11] provide examples of the pervasive private oversight over critical infrastructure.

Second, it restricts the scope of which countries' agendas matter in the making and shaping of cybersecurity—and which terms and institutional models are more desirable for conducting cyber operations.[12] With the United States, United Kingdom, European Union, China, and Russia as key players, one can often miss the specificities of how cyber operations and cyber norms are conceptualized and approached in other institutional contexts, more specifically, in Latin America.

Third, it positions countries beyond the great powers as either key adversaries or as "others," "secondary states," "developing states," "swing states,"[13] or "middle powers."[14] In this regard, such narratives can contribute to the fixing of a central position against which other countries are measured.[15] Such measurement can be identified more explicitly through the development of metrics to assess a country's maturity or cyber power,[16] and subjectively through discourses that seek to contrast authoritarian and democratic approaches.

In light of these challenges, the following section unpacks the role of regional bodies in attempting to build a common vision for tackling cybersecurity threats and Latin American countries' evolving position in the applicability of international law in cyberspace.

From regional developments to countries views on international cyber norms

For nearly two decades, the Organization of American States (OAS) has been a key player in promoting cybersecurity capacities in the region through technical trainings and dialogues and has become an important locus for member states to discuss cybersecurity-related issues at the regional level. In 2003, only two months after the adoption of the United Nations (UN) General Assembly resolution on the "Creation of a global culture of cybersecurity," the OAS published the "Declaración sobre Seguridad de las Américas," in which states recognize the need to adapt to a shifting threat landscape by establishing a multidimensional vision for hemispheric security. The declaration made explicit member states' commitment to identifying and combating "emerging threats" such as cybersecurity, biological terrorism, and threats to critical infrastructure.[17] The document also noted that states would develop a cybersecurity culture in the Americas by adopting measures for "preventing, treating, and responding to cyberattacks … combating cyber threats and cybercrime, typifying attacks against cyberspace, protecting critical infrastructure and protecting networked systems."[18]

While the 2003 Declaration was a critical step in setting a regional security vision that went beyond traditional threats and recognized the state was not the sole actor in providing security, the 2004 "Inter-American Strategy to combat threats to cybersecurity" further consolidated cybercrime and cybersecurity as an integral part of the hemispheric agenda. Since then, the agenda[19] has been operationalized through the work of the Inter-American Telecommunication Commission, the OAS Inter-American Committee Against Terrorism (OAS-CICTE), and the Meetings of Ministers of Justices, other Ministers, Prosecutors and Attorneys General of the Americas.[20]

In 2017 the OAS established, within CICTE, the Working Group on Co-operation and Confidence-Building Measures in Cyberspace (CBM). Member states have incrementally added new CBMs to the list.[21] These include, but are not restricted to, nominating points of contact at the policy level capable of discussing the implications of hemispheric cyber threats[22] and strengthening cyber capacity building through activities such as seminars, conferences, and workshops for both public and private sector officials in cyber diplomacy.

Despite the continuous regional efforts to deepen member state cooperation in cybersecurity and enhance cyber capacity building, when it comes to cyber operations, Latin American countries are still developing their own understanding of the topic. The fifth report of the Inter-American Judicial Committee (IACJ) on International Law and State Cyber Operations provides some insights into the present positions and gaps in defining cyber operations. The objective of the report was to improve "transparency with respect to how member states understand the application of international law to State cyber operations."[23] According to Duncan Hollis, the group rapporteur, states' legal capacities are uneven in this area. As he notes, "Some States evinced deep knowledge of cyber operations and the novel international legal issues they raise while others demonstrated much less familiarity with the underlying international legal rules and the particular questions their applications generate in the cyber context."[24] In addition, out of 35 OAS member states, only seven responded to the IACJ questionnaire.[25]

However, other forums, such as the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG)—all of which are part of the UN First Committee—pushed many member states to publish their views on the applicability of international law in cyberspace and their interpretation of what could be some of the "redlines" in the context of a cyberattack. As the table below shows, while many countries have not published an official document or developed views on state cyber operations and international law, they have provided some indications in OEWG speeches and interventions. The table presents excerpts from publicly available documents submitted by delegations in the occasion of the UNOEWG and the UNGGE.

Table: Latin American countries that published their views on cyber operations (emphasis added by the author)

Country	*Source*	*Declaration (extracted from documents/speeches)*
Brazil	*Comment on Initial Pre-Draft of the OEWG Report (2020)*	**Emphasis on electoral interference** "Brazil attaches fundamental importance to the need for adequate protection against threats to critical infrastructure, especially electrical, water and sanitation systems (paragraph 19). Electoral processes are also vulnerable to illegitimate interference through the malicious use of ICTs [Information and Communications Technology], and they should also be considered an essential component of the critical infrastructure of states."
	Comment on Zero Draft of the OEWG Report (2021)	"Brazil has a few specific text suggestions, especially in the section of international law, in which conceptual rigor is of utmost relevance. We will present our comments on each section as the debate evolves. We will also be glad to share with the chair`s team our specific comments to the text in written form."
	UNGGE Official Compendium (2021)	**Principle of sovereignty** "Interceptions of telecommunications, for instance, whether or not they are considered to have crossed the threshold of an intervention in the internal affairs of another State, would nevertheless be considered an internationally wrongful act because they violate state sovereignty. Similarly, cyber operations against information systems located in another State's territory or causing extraterritorial effects might also constitute a breach of sovereignty." **Use of force** The United Nations Charter does not refer to specific weapons or other means of use of force, and therefore the legal prohibition applies to all of them. Cyber operations may amount to an illegal use of force if they are attributable to a State and if their impact is similar to the impact of a kinetic attack.

Brazil	*UNGGE Official Compendium (2021)*	**Use of force—Recommendation on classification of cyberattacks to aid in interpretation of use of force and aggression.** "Although it is not binding, GA Res 3314(XXIX) has been considered highly authoritative and has guided the ICJ in its caselaw.3314 (XXIX) and cyber operations, due to their unique characteristics. Therefore, it is advisable to update the multilateral understanding of which acts amount to the use of force and aggression, so as to include instances of cyberattacks. In many instances, it might prove difficult to establish a direct analogy between the acts listed in GA Res." **State Responsibility - Attribution** [C]yber operations are attributable to a State if they are conducted by a state organ, by persons or entities exercising elements of governmental authority, or by persons or groups "acting on the instructions of, or under the direction or control of," the State. Regarding the latter criteria, for a private person or entity's conduct to be attributable to a State, it has to be proved that the state had "effective control" over the operations. It is clear, therefore, that a connection "must exist between the conduct of a [state] and its international responsibility."
Chile	*Comment on Initial Pre-Draft of the OEWG Report (2020)*	**Applicability of international law (IL), peaceful settlement of disputes, non-intervention.** "De la misma forma destacamos y apoyamos las menciones hechas respecto a que el derecho internacional y en particular a la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz y la estabilidad y promover un entorno de TICs abierto, seguro, estable, accesible y pacífico. También valoramos la mención a principios específicos de la Carta de las Naciones Unidas, en particular la solución pacifica de controversias, la prohibición de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o independencia política de cualquier Estado, la no-intervención en los asuntos internos de otros Estados, y el respeto por los derechos humanos y las libertades fundamentales." **Self-defense** "Por ejemplo, Chile considera legítimo la aplicación del principio de la auto-defensa en virtud del Articulo 51 de la Carta de las Naciones Unidas, si bien entiende que otros Estados discrepan."
	Comment on Zero Draft of the OEWG Report (2021)	--- (no mention of International Law or cyber operations) ---
Colombia	*Comment on Initial Pre-Draft of the OEWG Report (2020)*	**Applicability of International Law** "Colombia considers that general provisions and principles of international law could also apply to cyberspace and, at the moment, does not foresee the need to initiate negotiations for a new legally binding instrument on the subject."

Colombia	*Comment on Initial Pre-Draft of the OEWG Report (2020)*	**Attribution** "[D]iscussions regarding attribution of cyber-attacks at the UN level are welcome, in order to increase accountability for malicious cyber activities, and to determine the international responsibility of the States for their internationally wrongful acts in the use of ICTs." **Self-Defense** "The inherent right of individual or collective self-defense as recognized in the Charter of the United Nations is essential to maintaining peace and stability in the ICT environment, as it was confirmed by the 2015 GGE report." **Sovereignty** "State Sovereignty must not be used as a pretext to violate human rights and freedoms or tighten control over citizens. It is essential to maintain an open, secure, stable, accessible, and peaceful ICTs environment." **Regional collaboration** "Colombia supports the recommendation on enhancing the coordination with regional organizations, in order to exchange experiences at the UN level, on the development and operationalization of the confidence building measures and capacity building efforts."
	Comment on Zero Draft of the OEWG Report (2021)	**Applicability of International Law** "We highlight the importance of having the reference to the applicability of the existing international law in cyberspace, specifically of the United Nations Charter, as well as of leaving the door open for future dialogues related to its interpretation and application forms. The reference to the neutral and objective efforts for building capacities in this regard is fundamental." **Targets** "[M]y delegation celebrates the reference to the importance of the protection of critical infrastructure, which should include medical and healthcare facilities."
Mexico	*Comment on Initial Pre-Draft of the OEWG Report (2020)*	"The list of existing and emerging threats should also include the issues of hate speech and intrusive software, which were widely highlighted by Member States and stakeholders alike."
Uruguay	*Comment on Initial Pre-Draft of the OEWG Report (2020)*	**Sovereignty** "[T]he sovereignty of each State in the decisions to be taken and implemented in the future, as well as the guiding principles of the international law, must be respected without exception." **Human Rights** "The application of Human Rights norms in Cyberspace and for the use of information and communication technologies, especially the right to freedom of expression and online privacy, constitutes the pillars that the States must not ignore, but rather must guarantee and promote."

Uruguay	*Comment on Initial Pre-Draft of the OEWG Report (2020)*	**Non-intervention / neutrality** "Uruguay does not carry out or support activities that may damage the informational systems of the incident response centers in other States. It also does not carry out activities that seek to attack other centers from the CertUy."
Venezuela	*Comment on Initial Pre-Draft of the OEWG Report (2020)*	**Applicability of International Law** "Venezuela reiterates that the use of ICTs must be fully consistent with the purposes and principles of the UN Charter and international law, in particular the principles of sovereign equality, peaceful settlement of international disputes, refraining in international relations from the threat or use of force against the territorial integrity or political independence of any State, and non-intervention in the internal affairs of other States." [O]ur delegation recommends to avoid the mention made in paragraph three to the military use of cyberspace, and to abstain from making references to the application of international humanitarian law in this context, as said branch of international law is exclusive to armed conflict, as reflected in paragraphs 24 and 25. Inclusion of shared response and interpretations of violations Venezuela considers that this document should include a reference to the role of digital platforms, companies and States in assuring a responsible behavior that could prevent actions and/or attacks against the territories and critical infrastructure of other States, with a view to avoid the misuse of ICT's for hostile propaganda; interference in the internal affairs of States; violating the national sovereignty, security, public order and health systems of States; discriminatory treatment of information contents and/or disinformation; misuse for criminal and terrorist purposes. **Beyond malicious use of ICT** "The document should also contemplate a reference to the monopoly in internet governance, anonymity of persons, and aggressive cyber strategies which clearly affect the capacities of States." "Venezuela would like to see reflected a clear condemnation of the militarization of cyberspace and the covert and illegal use of computer systems to attack other States, as well as the proliferation of cybercrime and cyberterrorism, and an acknowledgement that further efforts are needed to promote an open, secure, stable and peaceful cyberspace from which all States can benefit, as well as effective and urgent measures, within the framework of international cooperation, to counter, by peaceful means, existing threats."
	Comment on Zero Draft of the OEWG Report (2021)	"Matters such as those relating to the automatic application of the UN Charter and the international responsibility of States for illegal acts in relation to the field of information and telecommunications in the context of international security lack consensus and could therefore be addressed in the text in a manner that effectively responds to the particularities and sensibilities of all Member States."

(Source: GGE[26]/OEWG)

As the table above shows, six countries from the region have published their statements on responsible state behavior in cyberspace in either the UNGGE or UNOEWG. In September 2021, Brazil was the only country in Latin America to have published an official document on these matters. While not all papers/speeches explicitly mention cyber operations, they provide some initial indicators regarding what could be considered a threat or risk to national cyber stability, including interference in electoral infrastructure (Brazil), attacks on human rights (Uruguay and Colombia), and the absence of a vision for a shared responsibility of malicious ICT acts (Venezuela).

Brazil's position paper provides more in-depth considerations of what would be understood as a cyber operation under the principle of the use of force. Brazil notes that "cyber operations may amount to an illegal use of force if they are attributable to a State and if their impact is similar to the impact of a kinetic attack."[27] Thus, the identification of a cyber operation is directly related to at least two criteria: first, a malicious attack that could fall under International Law includes those perpetrated by a state or a non-state actor. For a non-state actor to be associated with a state, "it has to be proved that the State had "effective control" over the operations."[28] In other words, the group or individuals involved should have been acting under the instructions or control of the state. However, many questions remain as to what kind of evidence would configure enough effective control to attribute state-sponsored hacking to a group. Second, Brazil highlights that a cyber operation is measured and understood not only in relation to the actor (attribution) but the intensity of its impact ("similar to the impact of a kinetic attack"), a position that has been shared by other states. Despite the country's public position, it is still unclear what circumstances would potentially trigger political attribution from Brazil and whether the government would consider – as others have done[29] – a more detailed distinction between 'scale' and 'effects' of the attack.

Countries in Latin America have been gradually developing their views on state cyber operations. However, the discussions around the applicability of international law in cyberspace represent only one dimension of a more complex landscape of defining cyber operations. In the case of international law, cyber operations are measured in relation to how and when they might trigger international law (attacks), what can be learned from customary international law, and how specific principles and protections under IL can support greater stability in the international system, and among other considerations. But what happens to all the activities below the threshold? How are they approached by countries in Latin America, and which bodies are responsible for responding?

The blurry (and dangerous) lines: cybersecurity and cybercrime in Latin America

For decades, cybercrime has been one of the main challenges facing countries in the region.[30] From the theft of financial data to cyber drug cartels, the threat landscape in Latin America combines the emergence of increasingly complex cyberattacks directed toward government bodies with the consolidation of organized crime online.[31] Financially motivated threats and ransomware attacks have become more sophisticated. If groups such as Anonymous were using distributed denial-of-service attacks in 2012 to take down websites from banking institutions in Brazil, the landscape in 2021 is much more complex.

In 2020, the North Korean group "BeagleBoyz" conducted a global campaign using remote access malware to steal data from financial institutions. Targeted countries in Latin America included Brazil, Chile, Costa Rica, Mexico, Panama, Peru, Uruguay, and Ecuador.[32] However, the attribution of BeagleBoyz as a state-sponsored group gained notoriety after the U.S. government issued a joint alert[33] on the group, associating it with Advanced Personal Threat 38:

> The BeagleBoyz overlap to varying degrees with groups tracked by the cybersecurity industry as Lazarus, Advanced Persistent Threat 38 (APT38), Bluenoroff, and Stardust Chollima and are responsible for the FASTCash ATM cash outs reported in October 2018, fraudulent abuse of compromised bank-operated SWIFT system endpoints since at least 2015, and lucrative cryptocurrency thefts. This illicit behavior has been identified by the United Nations (UN) DPRK Panel of Experts as evasion of UN Security Council resolutions, as it generates substantial revenue for North Korea. North Korea can use these funds for its UN-prohibited nuclear weapons and ballistic missile programs. Additionally, this activity poses significant operational risk to the Financial Services sector and erodes the integrity of the financial system.

Even though multiple Latin American countries were targeted, attribution was reportedly done by different bodies of the U.S. government—with incident responders in the region replicating the notification issued by the Cybersecurity and Infrastructure Security Agency (CISA).[34] Most countries in the region engage in attribution through public security bodies, such as the police, rather than political attribution of cyberattacks. Even so, it is important to note that although the latter can often be sparse, it does not mean it is non-existent. This was

the case in the aftermath of the Edward Snowden documents, when it was revealed that the United States had spied on President Dilma Rousseff and other important political leaders and Brazil openly called out the US for its cyber espionage.[35] Venezuela, on the other hand, has included cyber attribution as a growing part of their political strategy. Examples include the attribution of a major power outage in 2019 and an attack against the Bank of Venezuela – that left it offline for five days in 2021 – to the United States.[36]

Yet, even in the case of other notorious incidents, Latin American countries have often responded with a criminal approach[37] as the primary avenue for attribution and response. Governments across the region have been investing heavily in new programs for police forces and equipping them with tools for conducting forensic activities. Mexico, for example, launched a 24/7 network for cybercrime in 2017 and established a model for cybercrime police forces.[38] Other countries, like Brazil, also have a national network of cybercrime police stations.[39] The police have been working with other public security bodies, such as the Office of Integrated Operations (SEOPI) of the Ministry of Justice and Public Security on operational intelligence to investigate and respond to cyberattacks.[40] Even so, the development of institutional mechanisms dedicated to cybercrime has been followed by an increased acquisition of investigatory software and tools—often with little transparency regarding the purpose and continuity of the use of a specific tool. In the case of Brazil, a public call from the SEOPI for open-source software in May 2021 became a national conundrum when the bid received a proposal from the Israeli technology firm, NSO Group Technologies.

In early July 2021, multiple organizations such as Amnesty International, The Guardian, Forbidden Stories, and other media organizations came together to release the results of a months-long investigation into the use of the NSO Group Technologies' spyware solution, Pegasus.[41] Countries in Latin America, such as Mexico, had reportedly been using the spyware technology for more than a decade at the cost of over US$160 million to target groups.[42]

This emphasis on cybercrime has potential implications for understanding cyber operations as an integral part of criminal prosecution, technical attribution, and digital forensics activities. While the incipient discussion (or lack of one) on cyber operations at the regional level is partly tied to a lack of capacities or a mismatch of focal points at the national and regional levels, it can also serve as a smoke screen for Latin American countries to continue developing their cyber capabilities with little to no oversight. The blurriness between police forces and other public security bodies can (and has) posed challenges to accountability over software acquisitions. This is particularly worrying as it raises important questions over states' purchasing power of cyber weapons with a risk of little public oversight.

Conclusion

This paper sought to address how cyber operations and cyber norms are conceptualized in Latin America. To do so, regional and national developments in this field were reviewed, along with the involvement of countries in Latin America in international processes (UNGGE/OEWG).

The OAS continues to play an essential role in building cyber capacities in the region. However, as the IACJ report indicates, member states' views are still a patchwork of understandings about responsible state behavior in cyberspace and the role of cyber operations. One IACJ state representative called for "developing a distinctly Latin American perspective on the international governance and legal framework of cyberspace"[43] that would—instead of duplicating efforts—build on previous experiences (UNGGE and OEWG) to "develop a Latin American framework for understanding international law in cyberspace based on a shared political culture of democratic institutions and Ibero-American history." Comments such as this indicate some resistance to the great power rivalry and propose a complementary but Latin American interpretation of IL. [44]

However, as the paper highlighted, while Latin American countries face challenges in defining state cyber operations from an international law perspective. A more practice-oriented view of cyber operations indicates that some of their activities concentrate on the realm of cybercrime. Cyber operations, in its broader and practice-based sense, rely on concentrating capabilities in police forces and other public security bodies associated with law enforcement. This complex scenario points to a worrying landscape in which police forces and public security bodies can overextend their scope of activities through the acquisition of surveillance tools and other malicious solutions.

REFERENCES

[1] John R. Bolton, "Transcript: White House Press Briefing on National Cyber Strategy, September 20, 2018," *GrabieNews*,news.grabien.com/making-transcript-white-house-press-briefing-national-cyber-strateg.

[2] Jason Healey and Neil Jenkins, "Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing," *2019 11th International Conference on Cyber Conflict (CyCon) (2019): 1-20, doi.org/10.23919/CYCON.2019.8756890*.

[3] Caroline Levander and Walter Mignolo, "Introduction: The Global South and World Dis/Oder," *The Global South 5, no.1 (2011): 1-11, doi.org/10.2979/globalsouth.5.1.1*.

[4] Sean Aday, "Covering Cyber: Media Coverage of Cyber issues since 2014", *Institute of Public Diplomacy and Global Communication at George Washington University (2018): 1-17.*

[5] Lennart Maschmeyer, Ronald J. Deibert and Jon R. Lindsay, "A tale of two cybers–how threat reporting by cybersecurity firms systematically underrepresents threats to civil society," *Journal of Information, Technology and Politics 18, no.1 (2020):1-20*. https://doi.org/10.1080/19331681.2020.1776658.

[6] Patryk Pawlak and Panagiota-Nayia Barmpaliou, "Politics of cybersecurity capacity building: conundrum and opportunity," *Journal of Cyber Policy* 1, no. 4 (2017): 123-144, doi.org/10.1080/23738871.2017.1294610; and Andrea Calderaro and Anthony J. S. Craig, "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building," *Third World Quarterly* 41, no. 6 (2020): 917-938, doi.org/10.1080/01436597.2020.1729729.

[7] Matthew Kroenig, *The Return of Great Power Rivalry: Democracy vs Autocracy from the Ancient World to the U.S. and China (London: Oxford University Press, 2020).*

[8] United States, "Interim National Security Strategic Guidance," *White House, March 2021* https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf ; Cornell Overfield, "Biden's 'Strategic Competition' Is an Unclear, Confusing Term," *Foreign Policy, October 13, 2021,* https://foreignpolicy.com/2021/10/13/biden-strategic-competition-national-defense-strategy/.

[9] Louise Marie Hurel and Luisa Cruz Lobato, "Unpacking Cyber Norms: Private Companies as Norms Entrepreneurs," *Journal of Cyber Policy 3, no.1 (2018): 61-76.*

[10] Felipe Demartini, "Eletrobras e Copel são vítmas de ataques de ransomware," *CanalTech*, February 5 2021, canaltech.com.br/seguranca/eletrobras-e-copel-sao-vitimas-de-ataques-de-ransomware-178557/.

[11] Michael Schwirtz and Nicole Perlroth, "Darkside, Blamed for Gas Pipeline Attack, Says it is Shutting Down," *The New York Times, May 14, 2021,* www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html.

[12] Marsha Henry and Katherine Natanel, "Militarisation as diffusion: the politics of gender, space and the everyday," *Gender, Place & Culture* 23, no.6 (2016): 850-856, doi.org/10.1080/0966369X.2016.1164994.

[13] Tim Maurer and Robert Morgus, "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debates," *Global Commission on Internet Governance Paper Series No.2 (2014): 1-28,* www.cigionline.org/publications/tipping-scale-analysis-global-swing-states-internet-governance-debate-0/.

[14] Greg Austin, "Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security," *The Diplomat, February 2, 2016,* thediplomat.com/2016/02/middle-powers-and-cyber-enabled-warfare-the-imperative-of-collective-security/.

[15] This is not an exhaustive list of how the discourse and practices around the great power rivalry mandate other countries' engagement in cybersecurity. Calderaro and Craig (2020) note that from an international relations perspective, cyber capacity-building efforts have overly emphasized the concept of deterrence as a way to reduce cyber threats.

[16] See Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, and Anina Schwartzenbach, "National Cyber Power Index 2020," *Harvard Belfer Center, September 2020,* www.belfercenter.org/publication/national-cyber-power-index-2020.

[17] Organization of American States, "Declaración sobre seguridad en las Américas," October 28, 2003, www.oas.org/juridico/spanish/decl_security_sp.pdf, accessed September 07, 2021.

[18] OAS, "Declaración sobre seguridad en las Américas," 9-10.

[19] Maricarmen Sequera, Amalia Toledo, and Leandro Ucciferri, "Derechos Humanos y Seguridad Digital: uma Pareja Perfecta," www.tedic.org/wp-content/uploads/2018/06/DDHH-y-Seguridad-Digital-2-FINAL.pdf; and GFCE, "Overview of Existing Confidence Building Measures As Applied to Cyberspace," cybilportal.org/wp-content/uploads/2020/05/GFCE-CBMs-final.pdf, accessed August 30, 2021.

[20] That is not to say that the OAS' work in cybersecurity and cybercrime only started after the 2004 Inter-American Strategy to Combat Threats to Cybersecurity. A search through the OAS document databases indicates that one of the first documents to mention cybercrime (*delitos cibernéticos) in the context of REMJA, for example, dates back to 1999. The resolution notes the efforts of government experts in establishing a Justice and Cybercrime Studies Center for the Americas (AG/Res. 1615),* www.oas.org/juridico/english/ga-res99/

eres1615.htm. While most of the member states' work in this area have concentrated on CICTE, CITEL, and REMJA, other areas of the OAS, such as the Inter-American Commission on Human Rights, has continually tracked the relationship between cybersecurity and other rights, such as freedom of expression and rights infringements in the name of cyber operations. (See OAS, "CIDH y su Relatoría Especial manifiestan grave preocupación ante denuncias sobre espionaje a periodistas, defensores de derechos humanos, magistradas y dirigentes politicos en Colombia," www.oas.org/es/cidh/expresion/showarticle.asp?lID=2&artID=1162, accessed August 29, 2021).

[21] See GFCE, "Overview of Existing Confidence Building Measures As Applied to Cyberspace."

[22] Inter-American Committee Against Terrorism (CICTE) CICTE/RES. 1/18 (May 4, 2018): OEA/Ser.L/X.2.18.

[23] Inter-American Judicial Committee, "International Law and State Cyber Operations" (Washington, DC: OAS, August 2020), 5, www.oas.org/en/sla/iajc/docs/International_Law_and_State_Cyber_Operations_publication.pdf.

[24] Inter-American Judicial Committee, "International Law and State Cyber Operations."

[25] Responses to the questionnaire were complemented by additional statements from the OEWG and informal conversations in concert with consultations "held by the OAS Secretariat of the Inter-American Committee against Terrorism (CICTE) with the UN Office for Disarmament Affairs on August 15-16, 2019, and the informal intersessional meeting of the OEWG."

[26]Four OAS member states participated in the UNGGE 2019-2021: Brazil, Mexico, the United States, and Uruguay. However, only Brazil and the United States submitted their voluntary national contributions on how international law applies to cyberspace to be published in the official compendium of the UNGGE; this paper only considers Brazil, given its scope. UN General Assembly resolution 76/136, "Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communication technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution, A/73/266" (July 13, 2021), front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[26] UN General Assembly, "Official compendium of voluntary national contributions," 19.

[27] UN General Assembly, "Official compendium of voluntary national contributions," 21.

[28] Przemyslaw Roguski, "Application of International Law to Cyber Operations: A comparative analysis of states' views," *The Hague Program for Cyber Norms Policy Brief,* https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf?sequence=1&isAllowed=y, accessed 20 October 2021.

[29] Nir Kshetri, "Cybercrime and Cybersecurity in Latin American and Caribbean Economies," *Cybercrime and Cybersecurity in the Global South* (London: Palgrave Macmillan, 2013), 135–151.

[30] Robert Muggah and Pedro Augusto P. Francisco, "Drug Cartels are all over Instagram, Facebook, and TikTok," *Foreign Policy, December 15, 2020,* foreignpolicy.com/2020/12/15/latin-american-drug-cartels-instagram-facebook-tiktok-social-media-crime/.

[31] US CERT, "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," *CISA, August 26, 2020,* us-cert.cisa.gov/ncas/alerts/aa20-239a.

[32] CISA, FBI, USCYBERCOM, and the U.S. Department of the Treasury.

[33] MNEMO, "[Aviso de Seguridad] APT – Grupo de ciberdelincuentes "BeagleBoyz" dirige sus ataques a instituciones financeiras de todo el mundo," cert.mnemo.com/aviso-de-seguridad-apt-grupo-de-ciberdelincuentes-beagleboyz-dirige-sus-ataques-a-instituciones-financieras-de-todo-el-mundo/, accessed September 10, 2021.

[34] "EUA espionaram conversas de Dilma, diz TV," *BBC News*, September 2, 2013, www.bbc.com/portuguese/noticias/2013/09/130901_dilma_espionagem_fantastico_lgb.

[35] "Maduro atribui apagão na Venezuela a ataque hacker dos Estados Unidos," *globo.com G1*, March 9, 2019, g1.globo.com/mundo/noticia/2019/03/09/maduro-atribui-apagao-na-venezuela-a-ataque-hacker-dos-estados-unidos.ghtml; and "Venezuela acusa EUA de ataque a seu sistema financeiro," *CISO Advisor*, September 23, 2021, www.cisoadvisor.com.br/venezuela-acusa-eua-de-ataque-a-seu-sistema-financeiro/.

[36] Juan Carlos Garcia Caparros, "Top Cyber Threats to Latin America," *Mandiant,* May 24, 2021, www.mandiant.com/resources/top-cyber-threats-to-latin-america-and-the-caribbean.

[37] Government of Mexico, "Inician trabajos del Modelo Homologado de Polícias Cibernéticas," April 27, 2017, www.gob.mx/segob/articulos/inician-trabajos-del-modelo-homologado-de-policias-ciberneticas.

[38] "Delegacias Cibercrimes," *Safernet,* new.safernet.org.br/content/delegacias-cibercrimes#, accessed September 10, 2021.

[39] Government of Brazil, "Laboratório de Operações Cibernéticas do Ministério da Justiça e Segurança Pública auxilia operação contra ataques virtuais," *Ministério da Justiça e Segurança Pública,* www.gov.br/mj/pt-br/assuntos/noticias/laboratorio-de-operacoes-ciberneticas-do-ministerio-da-justica-e-seguranca-publica-auxilia-

-operacao-contra-ataques-virtuais, accessed September 10, 2021.

[40] Amnesty International, "Forensic Methodology Report: How to catch NSO Group's Pegasus," July 18, 2021, www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

[41] Avi Asher-Schapiro and Christine Murray, "INSIGHT-Pegasus spyware scandal: years of questions, no answers for Mexico victims," Reuters, August 9, 2021, www.reuters.com/article/mexico-tech-surveillance-idUSL8N2PD6BQ.

[42] OAS Inter-American Judicial Committee, "International Law and State Cyber Operations," www.oas.org/en/sla/iajc/docs/International_Law_and_State_Cyber_Operations_publication.pdf, accessed September 10, 2021.

[43] While there are many questions whether this alignment of visions will take place over the coming years, the IACJ has already presented a resolution calling for "training activities for various actors on the application of international law to cyberspace," Resolution CJI/RES. 259 (XCVII-O/20).

AUTHOR

Louise Marie Hurel is the Digital Security Programme Lead at Igarapé Institute, a think-and-do-tank focused on multidimensional security based in Brazil.