ARI 104/2020
15 September 2020

Balancing between giants, Latin-America's international cybersecurity position

Nathalie Van Raemdonck | Associate Analyst at the European Union Institute of Security Studies (EUISS) | @eilah_tan

Theme[1]

Latin American states have benefited from regional cooperation to improve their cybersecurity but are not leveraging this cooperation for issues of international peace and stability in cyberspace. This paper examines the region's international role and balancing exercise.

Summary

For the last few decades, Latin America has cooperated as a region on cybersecurity, and strengthened the capacity of states in the region to counter digital threats. While such regional cooperation could foster cyberdiplomacy convergence, Latin states have so far not formed a regional bloc in the conversations of the United Nations on the stability of cyberspace. The author finds that Latin states do however appear to share an approach to balance between major powers, walking a third way, providing examples from the region's relationship with the United States and China. Ultimately, Latin states appear to be primarily proponents of multilateral solutions to international cybersecurity issues with a primary role for the UN.

Analysis

Introduction

Latin America has enjoyed a long history of regional cooperation, ever since most countries won their independence 200 years ago. This is especially true for the peaceful resolution of conflicts. The most comprehensive cooperation happens through the Organization of American states (OAS), in which almost all North, Central, South American and Caribbean states are members. Throughout its history, trust in the OAS has fluctuated. During the Cold War period, the OAS was perceived more as an instrument of the dominance of the United States in which member states were forced to pick sides.[2] The need for alternative regional organisations without the US grew after the Cold War. The Community of Latin American and Caribbean States (CELAC) was the first regional mechanism to permanently group all 33 countries in Latin America without the United States and Canada. It aimed to be complementary to numerous

[1] This piece is based on a report written for EU Cyber Direct project funded by the European Union, 'Cyber Diplomacy in Latin America', https://eucyberdirect.eu/content_research/cyber-diplomacy-in-latin-america/.

[2] Detlef Nolte (2018), 'Costs and Benefits of Overlapping Regional Organizations in Latin America: The Case of the OAS and UNASUR', *Latin American Politics and Society*, 60(01).

ongoing sub regional projects and programmes. In the last few decades Latin American states have proclaimed the need to unite Latin America and face the challenges of globalization together. Such hopeful post-hegemonic regionalism, described by many scholars, has so far not delivered on its promise to establish a transnational sovereignty in the region. Latin American cooperation remains primarily applied to topical issues, rather than transgress to a broad political level. The Latin American efforts on creating security in cyberspace are characteristic of this process.

Regional cybersecurity

There have been several effective mechanisms in Latin America to exchange best practices and strengthen the region against digital threats, despite uneven levels of cyber development. Through the established cooperation under the OAS, Latin states already developed a regional cybersecurity strategy in 2004. Progress for the region as a whole has been slow ever since, likely due to a combination of factors – the lack of, and uneven levels of digital penetration; the low urgency for policymakers to coordinate their cybersecurity responses due to a lack of high-profile attacks; the lack of financial means to invest in digital security on a national level; a lack of expertise with policymakers and IT professionals. To overcome some of these challenges, the OAS' Inter-American Committee Against Terrorism (CICTE) created a specific "cybersecurity programme" for the region. The programme provides technical and operational support to OAS member states. It supports states in the development and implementation of a national cybersecurity strategy and organises regional cyber crisis exercises.

As Latin America is hardly one homogenous region but more composed of several subregions, progress has also been effective in recent years in the numerous trade cooperation. The Pacific Alliance's Digital Agenda Group and the meeting of authorities on information security and privacy and technological infrastructure of the Southern Common Market (MERCOSUR) have put cybersecurity on the trade cooperation's' agendas.

Latin America in the world

The regional progress on cybersecurity could create more unanimous positions on the international stage, even though Latin America rarely behaves like one bloc at the UN. The discussions in the OAS' cyber confidence building working group have the potential to align national interests among OAS members. While there are currently no such aspirations, they could form a regional cyber diplomacy strategy to build a secure and rights-based global cyberspace on an international level. CELAC as a cooperation mechanism also has the potential to unify positions at multilateral fora without the United States and Canada, and it provides CELAC member states with a stronger brokering position in the international field. Latin states however do not seem too intent on banding together on the international stage, and the regional cooperation mechanisms appear to have more practical/operational value than bring diplomatic convergence. Latin America might be perceived as a regional bloc as there is conformity between most countries in the region to pursue a middle ground in geopolitical debates. With the recollection of the Cold War still fresh, the motivation to avoid becoming a frontier in a trade war that might split the internet is high. So is the motivation to protect the internet from becoming the next military battleground. This is particularly important in a region where the digital

revolution has started to bring socio-economic benefits. This means Latin countries are positioning themselves more in a 'third-way', independent but friendly with all major powers in the world. The relationships of Latin states with the Unites States and China are symptomatic of this balancing act.

A strained American marriage

Latin America has historically been intertwined with the United States, and this has been no less true for digital issues. Latin states are however changing the US' role in the region when it comes to cyberspace. First, countries on the continent are reducing their dependency on the infrastructure of the United States. The construction of a submarine cable connecting Latin America with Europe, the EllaLink cable, is expected to significantly decrease their traffic dependency on the United States. States are also exploring the potential for a Trans-Pacific internet cable, as proposed by former Chilean President Bachelet at the 2018 CELAC-China summit. The global surveillance operations conducted by the National Security Agency (NSA) of the United States discovered in 2013 with the Snowden revelations, awoke Latin states and their populations to the need for building secure and independent telecommunications network. This opposition to foreign surveillance was also vocalized at the United Nations in 2013.[3] A second point of the changing relationship is the international discontent. Latin states are not falling in line with their regional partner when it comes to international discussions on cyberspace. Most Latin states voted for the establishment of the Open-Ended Working Group (OEWG) at the United Nations to discuss cooperation on stability in cyberspace. This was much to the dismay of the United States, who saw the Russia-sponsored OEWG proposal as competing to its proposal for the creation of a new UN Group of Governmental Experts.[4]

Some Latin states, such as Brazil[5], Peru[6] and Cuba[7], have also expressed unease over the use of offensive capabilities in cyberspace and warned against the militarization of the information and communication technologies (ICT's). This perspective contrast with the "persistent engagement" strategy of the United States with which it seeks to operate

[3] United Nations General Assemblee, Statement by H.E. Dilma Rousseff, President of the Federative Republic of Brazil at the Opening of the General Debate of the 68th Session of the UNGA, 2013, https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

[4] Alex Grigsby (2018), 'The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', *Net Politics*, Council on Foreign Relations, 15/XI/2018, https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

[5] Brazil's statement 'Weaponisation of ICT tools increases the unpredictability in international relations. Recognition by the UNGGE report of the applicability of international law is not a legitimisation of cyberconflict, nor would it be incompatible with the objective of preventing the breakout of cyber warfare' at the UN Open Ended Working Group 1st substantive session, https://dig.watch/resources/2nd-meeting-first-substantive-session-open-ended-working-group-oewg.

[6] Peru's statement 'Peru expressed concern that states are developing their ICT capacities towards military ends' at the UN Open Ended Working Group 1st substantive session, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/statements/10Sept_Peru.pdf.

[7] Cuba's statement 'Attempts to make cyberspace a theatre of military operations must be rejected' at the UN Open Ended Working Group 2ndst substantive session, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/statements/10Feb_Cuba.pdf.

militarily in cyberspace within the confines of international law. A third point of the changing relationship is the pursuit of trade cooperation with different regions. The European Union-MERCOSUR Free Trade agreement was finalised in 2019 after being at a stalemate for 20 years. The Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) created one of the largest free trade zones in 2018 with 11 countries across the Pacific.[8] When the United States withdrew from its predecessor, the Trans-Pacific Partnership (TPP), it gave up a strategic advantage in the region against China. This point also speaks of the increasing level of disregard of the United States for the region under President Trump. For example, there was no president of the United States present at the 8th OAS Summit of the Americas in Lima in 2018. This was a first. Ironically, and also for the first time ever, there was a Chinese delegation present at that summit. Many of the economic interests of the United States are safeguarded through bilateral free trade agreements with various Latin American countries,[9] but it is becoming obvious that the region is diversify its trade and exploring new partnerships, among others with China.

The Chinese connection

China has significantly expanded its presence in Latin America since 2000. Trade has multiplied 18 times between 2000 and 2016 and China has become the region's second-largest trading partner.[10] Both the MERCOSUR and Pacific Alliance trading blocs have generally welcomed China's trade and investment in Latin America. At the 2018 China-CELAC summit, China extended an invitation to countries in the region to become part of its Belt and Road initiative, which several Central American and Caribbean countries appear to have accepted.[11] There is however risk of value distortion that comes with cooperation and trade with a partner that does not have the best track record on human rights. Some of the more developing countries, specifically in Central America, are receiving cheap electronic equipment and have accepted Chinese support for increased digitalisation. Part of that support is coming in the form of surveillance technology that is adapted to China's political system. Ecuador's new police system, for example, was largely made by the Chinese state-controlled CEIEC and Huawei. Replicas are also being sold to Bolivia and Venezuela, and Argentina also seems eager to buy into Chinese surveillance technology. While Chinese expertise and loans can jumpstart e-commerce, there is unease over the increasing presence of Chinese infrastructure in the region. Civil society organisations in Latin America are worried[12], especially in light of the

[8] Partner countries are Australia, Brunei, Japan, Malaysia, New Zealand, Singapore, Vietnam, Peru, Mexico, Chile and Canada.

[9] Bilaterally with Chile (2004), Peru (2009), Colombia (2012) and Panama (2012), and multilateral (2009) with the Dominican Republic Republic and the Central American states of Costa Rica, El Salvador, Guatemala and Nicaragua (Dominican Republic-Central America Free Trade Agreement (DR-CAFTA).

[10] Anabel Gonzalez (2018), 'Latin America-China Trade and Investment Amid Global Tensions', The Atlantic Council's Adrienne Arsht Latin America Center, December 2018, https://www.atlanticcouncil.org/wp-content/uploads/2018/12/Latin America-China-Trade-and-Investment-Amid-Global-Tensions.pdf

[11] Juan Enrique Serrano Moreno, Diego Telias and Francisco Urdinez (2020), 'Deconstructing the Belt and Road Initiative in Latin America', *Asian Education and Development Studies*, June 2020.

[12] Maricarmen Sequera, Amalia Toledo and Leandro Ucciferri (2019), 'Derechos Humanos y Seguridad Digital: Una Pareja Perfecta. Aportes de la sociedad civil hacia políticas nacionales de seguridad digital (cont.)

recent COVID-19 pandemic. China has built digital solutions to combat the pandemics that are far from being respectful of human rights. Digital rights organisations have warned of the possible application of these tools by Latin American states.[13]

A 'Third Way'?

A rapprochement with China might be worrying, but identification with liberal values still appears to prevail in the governments and active citizenship in Latin America.[14] There remains a commitment of the region to principles of a free, open and rule-based Internet. It is however visible how countries in the region have been in balancing act between giants in an exercise that echoes the polarized world during the Cold War. This time, Latin states seem to be more successful in avoiding exploitation and even attempting to benefit from these relationships. They are also not alone in this balancing act. The call for a 'third way' for cyberspace was loudly uttered at the 2018 launch of the Paris Call. As French president Emmanuel Macron described it, the Paris Call sought to find support for a middle ground between an authoritarian Chinese and a Silicon Valley internet whose algorithmically biased platforms may not provide a healthy online media environment. The Paris Call reiterates the principles established over almost a decade of work by multilateral and multi-stakeholder fora.[15] It was endorsed and supported by Mexico, Chile, Colombia, Argentina, Peru, and Panama.[16]

Europe's concept of a 'third way' seems to consists of the establishment of rules for any industry engaged in the region, as is evident from the creation of the General Data Protection Regulation (GDPR), the cybersecurity Act and 5G industry regulations[17], or from imposing sanctions against entities and individuals involved in cyber-attacks. The regulatory power of the European Union is not easy to replicate in other regions in the world, and it is also not always welcomed. The European decisions have an impact on the rest of the world but were only negotiated by the member states of the European Union. Latin-America's middle ground approach for cyberspace focuses primarily on the multilateral stage. For example, Mexico proposed the creation of a working group in the International Law Commission (ILC) at the Second Substantive Session of the OEWG.

que respeten y protejan los derechos humanos', TEDIC, Asociación por los Derechos Civiles (ADC) and Fundación Karisma, January 2019, https://www.tedic.org/wp-content/uploads/2018/12/InformeCiberseguridadParte1.pdf.

[13] For example the Mexican Network in Defense of Digital Rights (R3D) gathered support from 11 Latin Civil Society organisations to sign its call to Latin American governments that digital technologies applied to the covid-19 pandemic respect human rights,warning for the influence of Chinese solutions, https://r3d.mx/2020/03/20/sociedad-civil-covid-19-ddhh/.

[14] Andrés Serbin and Andrei Serbin Pont (2019), 'Why should the European Union have any relevance for Latin America and the Caribbean?', EU-LAC foundation, 30/IV/2019.

[15]Arthur P.B. Laudrin (2018), 'Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace', *Lawfare Blog*, 04/XII/2018, https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace.

[16] France Ministry for Europe and Foreign Affairs, 'Paris Call of 12 November 2018 for Trust and Security in Cyberspace', 12/XI/2018, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[17] Annegret Bendiek and Martin Schalbruch (2019), 'Europe's Third Way in Cyberspace, What Part Does the New EU Cybersecurity Act Play?', *SWP Comment* 2019/C 52, December 2019, https://www.swp-berlin.org/10.18449/2019C52/.

This could produce a study on the applicability of current international law in cyberspace, complementary to national positions.[18] Similar exercises had so far only taken place under the auspices of the North Treaty Alliance Organization (NATO) who created the Tallinn manual on the international law applicable to Cyber Operations. Latin states also proposed an implementation mechanism for cybernorms at the 1st session of the Open-ended Working Group.[19] In this mechanism, member states of the United Nations should be able to make periodic national reporting on how they have implemented the agreed rules, norms, and principles. The Secretary General would compile national responses, providing a central role to the United Nations.

Conclusion

Considering these actions, Latin America's balancing act becomes apparent. Practical advancement can spring from regional cooperation and walking a middle ground must benefit the countries in the region, but from the perspective of Latin America, the future of international cybersecurity is multilateral. If it were up to Latin America, a balance must be upheld in decision-making over a rule-based cyberspace, to maximise the socio-economic benefits of the internet for society.

[18] Mexico's 2020 proposal at the 2nd substantive Open Ended Working Group session for the Study of the ILC on the applicability of international law in cyberspace, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/mexico-study-of-the-ilc-applicability-of-international-law-in-cyberspace.pdf.

[19] Mexico's 2019 proposal at the 1st substantive Open Ended Working Group session for a follow-up implementation mechanism, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/mexico-follow-up-implementation-mechanism-proposal.pdf.