DIGITAL DIALOGUE

Cyber Diplomacy in Latin America

Nathalie Van Raemdonck
EU Institute for Security Studies
June 2020

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

Contents

Abstract 4

Key takeaways 4

1. General regional profile 5

2. Latin America as a region: the institutional landscape 7
2.1. Regional organisations 7
2.2. Non-governmental organisations 10

3. Policy issues, priorities, and actions 13
3.1. Cooperating on resilience 13
3.2. Fight against cybercrime 15
3.3. Building confidence 17
3.4. Protecting democracy 18
3.5. Boosting the digital economy 20
3.6. Military cyber presence 21

4. Regional approaches to cyber diplomacy and resilience 22
4.1. The international law and norms debate 22
4.2. Cybercrime 26
4.3. Free and open rule-based internet 27

5. Navigating between the US and China 28
5.1. United States 28
5.2. China 29

6. The EU and Latin America 30
6.1. Strategic partnership with the EU 31
6.2. Cyber cooperation 32

Conclusions 36

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author.

Abstract

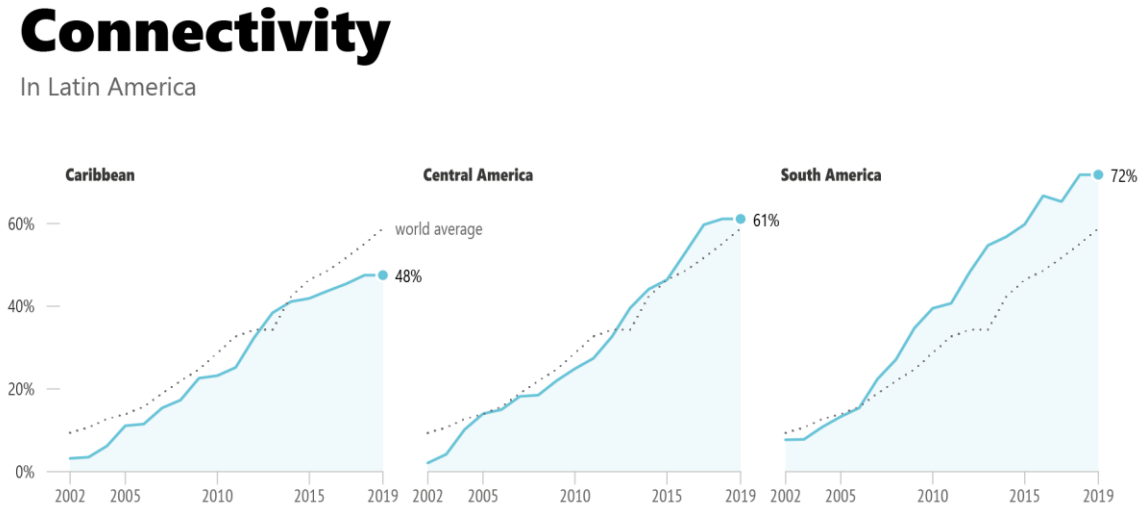
Latin America is an important region for the EU to build a secure and rights-based global cyberspace. Despite tumultuous political transitions in the past few decades, Latin America has been a staunch defender of liberal values and inclusivity, both in the digital sphere and in the physical realm. Latin states became the first in the world to coordinate their efforts on cybersecurity in 2004 with a cybersecurity strategy. Under the Organisation of American States (OAS), numerous cybersecurity initiatives were created for the region. This digital dialogue provides an overview of the regional cooperation and Latin American efforts to increase resilience, create confidence building measures, fight cybercrime, boost the digital economy, and protect human rights online. It dissects the Latin American position in the world on cyber diplomacy and how it positions itself towards the US, China, and the EU to create stability in cyberspace. Specific attention goes to the strategic partnership between the EU and Latin America and how this relationship can be leveraged to increase cooperation to foster global stability in cyberspace.

Key takeaways

- Despite changing alliances and clashing ideologies in Latin America, there are effective regional cooperation mechanisms that strengthen the region against digital threats. The OAS' cybersecurity programme and Confidence-Building Working Group contribute greatly to this effective cooperation.
- While Internet freedom seems to be declining in the region, Latin countries have expressed a commitment to liberal values in international fora. There is great potential in the region for developing Internet governance models that involve multiple actors with active civil societies and emerging digital economies.
- Many Latin states have expressed views similar to the European Union, e.g. that the Internet needs to remain free and open and that a secure cyberspace needs to be rules-and rights-based. They have expressed the need for a clear dialogue on the application of international law in cyberspace and several Latin states have pleaded for the United Nations to play a greater role in implementing cybersecurity norms.

1. General regional profile

Latin America is an important region for the EU to build a secure and rights-based global cyberspace. Despite tumultuous political transitions in the past few decades and rampant inequalities, Latin America has been a staunch defender of liberal values and inclusivity, both in the digital sphere and in the physical realm. In the last few decades, the region has increasingly adapted its societies to the digital reality. Well over two-thirds of the population in Latin America is now online, compared to only 53.6 percent of Internet users globally, according to International Telecommunication Union (ITU) figures.[1] According to a recent estimate, 72 percent of the population in South America, 61 percent in Central America, and 48 percent in the Caribbean now have direct access to the Internet.[2] There is an untapped potential for more digital penetration in the region, which comes with an urgency to secure the next generation of Internet users.



Data: Internetworldstats.com, ITU

With increasing connectivity comes increasing vulnerability. A few facts on threat actors and vulnerabilities paint an interesting picture of Latin America's cybersecurity landscape.

- According to the OAS Inter-American Development Bank (IDB) 2016 report, **cybercrime** cost Latin America **$90 billion**, out of a worldwide $575 billion.[3] From a more recent study, it seems the annual cost of cybercrime has reached $8 billion in Brazil, $3 billion in Mexico, and $464 million in Colombia, which constitute the worst affected countries in the region.[4]
- The financial sector is heavily targeted in Latin America, with a 2018 OAS report confirming **that 9 out of 10 banks** have been targeted by a cyberattack. Of these, 37 percent confirm

1 International Telecommunications Union (2019) ICT Facts and Figures. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf
2 Internet World Stats (2019) The Caribbean https://www.Internetworldstats.com/carib.htm Mexico and Central America https://www.Internetworldstats.com/central.htm South America https://www.Internetworldstats.com/south.htm
3 Organization of American States (OAS) Inter-American Development Bank (IDB) (2016) 'Cybersecurity: are we prepared in Latin America and the Caribbean'
4 Center for Strategic and International Studies and McAfee (2018) Economic Impact of Cybercrime – No slowing down" https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

they were the victim of a successful cyberattack - ultimately costing Latin American banks approximately $809 million in 2017.[5]

- Cybercrime mostly emanates from the region itself, with Brazil and Mexico being the leading **sources of online attacks** in Latin America.[6] Brazil is also known worldwide for housing huge botnets.[7] Brazilian-bred financial malware has become highly effective in targeting the Spanish-speaking world.[8]
- Cybercrime in Latin America has varying degrees of complexity and the **professionalisation of cybercrime groups** in Latin America is worrying, according to Kaspersky Labs, which tracks threat actors.[9]
- **Mobile malware** is also very prevalent in the region, which is concerning considering more than half of Internet traffic in Latin America comes from a mobile device.[10]
- Latin American digital consumers visit or update social media platforms more often than the rest of the world, which means there is a bigger attack surface for threats such as **social media scams, disinformation, and identity theft**.[11]
- Latin American countries have seen relatively low amount of threats from **nation state actors**. The most notable nation state attack was the global WannaCry ransomware attacks in 2017. Mexico and Brazil were the biggest victims in the region; Mexico was even the fourth worst affected country globally.[12]

Latin American states and their citizens became increasingly aware of their online footprint following the Snowden leaks that revealed the United States' global surveillance operations in 2013. This awoke Latin states and their populations to the potential threats in the digital realm. Latin nations made statements at the United Nations, individually and through the regional organisations CELAC and UNASUR, regarding the surveillance operations.[13] Then-Brazilian President Dilma Rousseff condemned the practices and called for multilateral mechanisms for the governance and use of the Internet that ensured human rights and respected national sovereignty.[14] As a direct consequence, Brazil organised the NETmundial conference together with ICANN in 2014, a global multi-stakeholder meeting on the future of Internet governance that was the first "experiment" of its kind coming from the region.[15]

---

[5] Organization of American States (OAS) (2018) 'State of Cybersecurity in the Banking Sector in Latin America and the Caribbean'

[6] Center for Strategic and International Studies and McAfee (2018) 'Economic Impact of Cybercrime – No slowing down' https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

[7] Spamhaus Project keeps an updated list of 'The World's Worst Botnet Countries' last accessed 13/02/2020 https://www.spamhaus.org/statistics/botnet-cc/

[8] Cyberreason (2018) 'Pervasive Brazilian Financial Malware targets banking customers in Latin America and Europe' https://www.cybereason.com/blog/brazilian-financial-malware-banking-europe-south-america

[9] Kaspersky Global Research & Analysis Team (2018) 'Bingo, Amigo! Jackpotting: ATM malware from Latin America to the World', *Securelist*

[10] Threatmetrix (2018) 'Latin American Cybercrime Trends' https://www.threatmetrix.com/digital-identity-blog/cybercrime/Latin American-cybercrime-trends-attacks-increase/

[11] Threatmetrix (2018) 'Latin American Cybercrime Trends' https://www.threatmetrix.com/digital-identity-blog/cybercrime/Latin American-cybercrime-trends-attacks-increase/

[12] Kaspersky Global Research & Analysis Team (2017) 'Después del WannaCry en Latinoamérica' https://securelist.lat/despues-del-wannacry-en-latinoamerica/85056/

[13] Individual statements were made by Brazil, Ecuador, and Venezuela, and Cuba spoke on behalf of the CELAC at the 68th UNGA, whereas Suriname spoke on behalf of the UNASUR at the 2013 1st Committee sessions

[14] United Nations General Assemblee (2013) "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" https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf

[15] Geneva Internet Platform (2014) "Why NETmundial mattered and what was achieved" https://www.giplatform.org/resources/why-netmundial-mattered-and-what-was-achieved

The views expressed at the UNGA for the first time in 2013 in support of a free, open, secure, and rule-based cyberspace have persisted and largely run parallel to the EU's cyber diplomacy stances in international fora. This perception of ideological convergence will however be put to the test in the following years, when states will need to start implementing those values and obligations on a domestic level.

Increasing resilience and halting cybercrime have been high on Latin America's agenda to increase stability in cyberspace. Twelve countries have created a national cybersecurity strategy and most are in the process of working on a strategy with the support of the OAS and its regional cybersecurity programme. Latin America, however, got a headstart: The OAS was the first region in the world to formulate a cybersecurity strategy in 2004. Progress has been steady but slow ever since, likely due to a combination of factors - low urgency for policymakers, lack of financial means to invest in digital security, lack of expertise with policymakers and IT professionals, lack of high-profile attacks, and a lack of leadership in the region.

2. Latin America as a region: the institutional landscape

The institutional landscape in Latin America is made up of several regional organisations that shape regional development and several non-state actors that engage in multi-stakeholder discussions. A deeper look at the historic transformations of Latin America's regional organisations is useful for understanding how the region builds political consensus. A mapping of those organisations and their membership paints a better picture of the alliances and convergences in the region.

2.1. Regional organisations

Latin America has enjoyed a long history of regional cooperation, since most countries won their independence 200 years ago. This is especially true for the peaceful resolution of conflicts.[16] The Western Hemisphere has engaged in security cooperation for a long time through the OAS, which also includes Canada and United States. The OAS was founded in 1948, following the 1947 Inter-American Treaty of Reciprocal Assistance (TIAR), also known as the Rio Treaty, in which all North American and Latin American countries pledged to a hemispheric defence doctrine of collective security.[17] The OAS has been the strongest and best established cooperation organisation for the region. Throughout its history, trust in the OAS has fluctuated. During the Cold War period, the OAS was perceived more as an instrument of US dominance in which member states were forced to pick sides.[18] Faith in the collective security doctrine plummeted when the US favoured the UK over Argentina during the Falkland War.[19] In the last few decades, Mexico, Bolivia, Ecuador, Nicaragua, and Venezuela even withdrew from the Rio Treaty. American intentions on democracy in Latin America have been scrutinised during the coup in Chile in 1973, the failed coup against former Venezuelan President Chavez in 2002 and the support for

[16] Kurtenbach, Sabine (2019) 'Latin America – Multilateralism without Multilateral Values' Giga Focus, 2019-7

[17] Organisation of American States (OAS) 'Inter-American Treaty of Reciprocal Assistance (Rio Treaty)' entry into force 12 March 1947 http://www.oas.org/juridico/english/treaties/b-29.html

[18] Nolte, D. (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)

[19] Sennes, Ricardo; Onuk, Janina; de Oliveira, Amacio Jorge (2006) 'The Brazilian foreign policy and the hemispheric security' *Center for International Negotiation Studies* n.3-4, p.3-26

the transitional government in Honduras in 2009, which showed the US' preferences for securing economic and strategic interests over liberal norms and values.[20] The OAS also has a complicated history with Cuba and Venezuela, which are currently refusing to participate in the organisation.[21]

The need for an alternative regional organisation without the US grew during the "posthegemonic regionalism" phase after the Cold War. This began with the "pink tide", a political left turn by many Latin American governments in early 2000.[22] Political alliances like CELAC, UNASUR, the Andean Community, and ALBA were formed in the new millennium with economic, social, and political integration goals. These organisations have a security agenda and some of them have also created working groups on digital issues. Both CELAC and UNASUR have made some declarations on the governance of cyberspace, stressing the protection of national sovereignty while maintaining a free flow of information.[23]

The Community of Latin American and Caribbean States (CELAC) became the official counterpart for region-to-region diplomatic dialogue with the European Union when it was created in 2011.[24] CELAC was the first regional mechanism to permanently group all 33 countries in Latin America without the US and Canada. It aimed to be complementary to numerous ongoing subregional projects and programmes. As a regional forum rather than an organisation, it mostly strived to coordinate actions and provide space for political consultation.[25] However, the humanitarian crisis in Venezuela significantly strained cooperation. A split has arisen in organisations like CELAC and UNASUR in recent years, and countries like Cuba, Nicaragua, and Bolivia have taken Venezuelan president Maduro's side.[26] UNASUR, the Union of South American Nations, imploded in late 2018. Most members suspended their membership in 2019. A new alliance, the PROSUR, was created in 2019 without Venezuela under the leadership of Chilean President Piñera and Colombian President Duque.[27]

[20] Kurtenbach, Sabine (2019) 'Latin America – Multilateralism without Multilateral Values' Giga Focus, 2019-7

[21] Venezuela started the process of withdrawing from the OAS entirely for not abiding to the Inter-American Democratic Charter under president Maduro, but remains a member after the takeover by interim president Juan Guaido. Cuba was a founding member but was excluded from participating between 1962 and 2009. While Cuba was reinstated in 2009 to participate, it has chosen not to return to the OAS. Kurtenbach, Sabine (2019) 'Latin America – Multilateralism without Multilateral Values' Giga Focus, 2019-7

[22] Castro, Rafael & Lenz, Tobias (2019) 'The Lima Summit: a Trial by Fire for the Pacific Alliance' GIGA Focus 2019-4

[23] Community of Latin American and Caribbean States (CELAC) (2015) 'Special Declaration 15 of the CELAC on Internet gobernance process' 2015 CELAC Summit in Costa Rica

UNASUR (2013) 'Paramaribo Declaration adopted at the VII UNASUR summit' http://www.itamaraty.gov.br/en/press-releases/5337-paramaribo-declaration-adopted-at-the-vii-unasur-summit-paramaribo-august-30-2013

[24] European External Actions Service (2018) "EU-CELAC relations" https://eeas.europa.eu/headquarters/headquarters-homepage_en/13042/EU-CELAC%20relations

[25] Stevens, Christine (2015) 'Region to Region Cooperation: EU and CELAC' Egmont Institute

[26] Castro, Rafael & Lenz, Tobias (2019) 'The Lima Summit: a Trial by Fire for the Pacific Alliance' GIGA Focus 2019-4

[27] The signatories to the PROSUR Santiago declaration are Argentina, Brazil, Colombia, Chile, Ecuador, Guyana, Paraguay, and Peru. Government of Peru (2019) 'Declaración Presidencial sobre la Renovación y el Fortalecimiento de la Integración de América del Sur' https://www.gob.pe/institucion/rree/noticias/26812-declaracion-presidencial-sobre-la-renovacion-y-el-fortalecimiento-de-la-integracion-de-america-del-sur

CELAC, as a cooperation mechanism, also went through a rough patch. There were no CELAC summits organised in 2018 and 2019 under the respective El Salvadorian and Bolivian presidencies. Mexico assumed the presidency in 2020, expressing its commitment to strengthen CELAC as a cooperation mechanism for the 33 member countries, and to position CELAC on the international stage.[28] The first CELAC summit during the Mexican presidency was organised in January 2020, which observers called a "third way" approach between supporters and opponents of Venezuela's former and interim governments.[29] Notable absentees from the 2020 CELAC summit were Bolivia and Brazil. The Bolivian interim government protested the asylum Mexico granted to former President Evo Morales, while the Brazilian government decided to pull out of the organisation they claimed was "a stage for authoritarian states".[30] While there was no mention of digital issues in CELAC's 2020-2021 workplan, the objective to strengthen the unity of CELAC countries in multilateral forums can have an impact on the region's participation in Internet governance discussions.

In the 2010s, a "blue tide" of right-wing conservative presidents also rose in Latin America, who increased their focus on trade.[31] To be sure, trade cooperation was a priority before this blue tide, most notably with the Southern Common Market, also known as MERCOSUR, which initially had a more social focus. The trade bloc, created in 1991, stressed the importance of trade for social development. The blue tide, meanwhile, consolidated a "trade turn" towards prioritising the enlargement of the market and attracting foreign investment. This converged with the objectives of the more recent Pacific Alliance. This trade block formed around 2011 to unite Latin countries on the Pacific coast with a focus on trade with Asia.[32] Heads of state of MERCOSUR have usually been present at Pacific Alliance summits and members seem favourable towards convergence of the two trade blocks.[33] There are economic incentives in both MERCOSUR and the Pacific Alliance to improve cybersecurity and both organisations

[28] Gobierno de México (2020) 'Foreign Secretary Ebrard Presents Mexico's Work Plan as CELAC President Pro Tempore' Press release https://www.gob.mx/sre/prensa/foreign-secretary-ebrard-presents-mexico-s-work-plan-as-celac-president-pro-tempore?idiom=en

[29] Garcia, Jacobo (2020) 'La CELAC deja fuera las crisis de Venezuela y Bolivia en la primera reunión bajo el liderazgo de México' https://elpais.com/internacional/2020/01/08/mexico/1578520081_860089.html

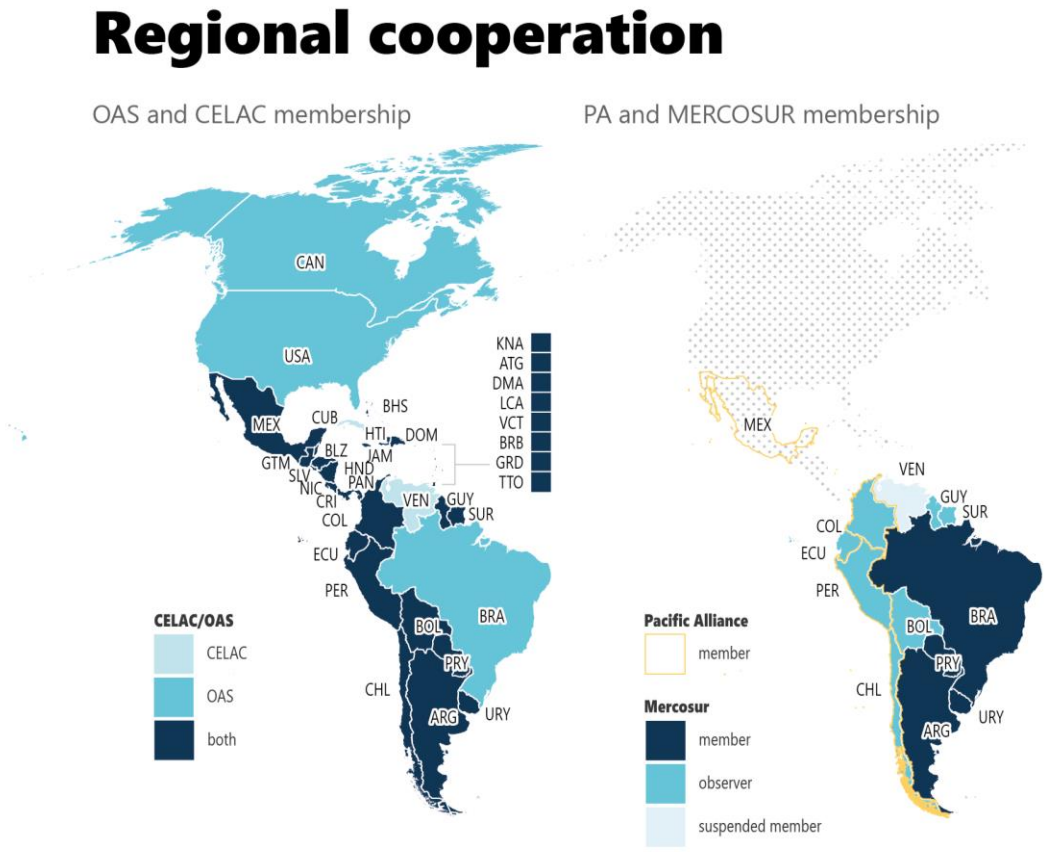
[30] Reuters (2020)'Brazil sits out leftist Latin American nations' body on anti-democracy fears' https://www.reuters.com/article/us-brazil-diplomacy-celac/brazil-sits-out-leftist-Latin American-nations-body-on-anti-democracy-fears-idUSKBN1ZF2U9

[31] Castro, Rafael & Lenz, Tobias (2019) 'The Lima Summit: a Trial by Fire for the Pacific Alliance' GIGA Focus 2019-4

[32] Castro, Rafael & Lenz, Tobias (2019) 'The Lima Summit: a Trial by Fire for the Pacific Alliance' GIGA Focus 2019-4

[33] Marczak, Jason (2018) 'Latin America's Future Begins with the Pacific Alliance' Atlantic Council https://www.atlanticcouncil.org/blogs/new-atlanticist/Latin America-s-future-begins-with-the-pacific-alliance

are in the process of developing a digital agenda that includes cybersecurity. In the regional context, this brings a different set of actors to the regional security debate. Expectations should be kept low for now, as plans to increase resilience are in an outline stage in both organisations.[34]



2.2. Non-governmental organisations

Non-governmental organisations are an important part of Latin American decisionmaking processes. Receptiveness to contributions of non-state actors was first conceptualised in the OAS' updated security doctrine in 2003.[35] In this doctrine, the OAS recognised that security challenges are multidimensional paradigms in which a diversity of actors converge: state, non-state, and supranational actors.[36] The OAS has actively sought the engagement of private industry and the technical community for its cybersecurity programme. It tries to involve local private industry when providing assistance for the development of national cybersecurity strategies.[37]

[34] Pacific Alliance: Digital Agenda (last accessed 04/07/2019) https://alianzapacifico.net/en/technical-group-digital-agenda/
[35] Organization of American States (OAS) (2003) 'Declaration on Security in the Americas' CES/DEC.1/03 rev. 1
[36] Sequera, Maricarmen; Toledo, Amalia & Ucciferri, Leandro (2018) "Derechos Humanos y Seguridad Digital: Una Pareja Perfecta. El rol de organizaciones multilaterales en la agenda latinoamericana de seguridad digital, El caso de la OEA" TEDIC, la Asociación por los Derechos Civiles (ADC), Fundación Karisma https://www.tedic.org/wp-content/uploads/2018/06/DDHH-y-Seguridad-Digital-2-FINAL.pdf
[37] Organization of American States (OAS) (2015) 'OAS Cybersecurity Initiative' presentation prepared for the Global Forum on Cyber Expertise (GFCE) https://www.sites.oas.org/cyber/Documents/2015%20OAS%20Cybersecurity%20Initiative.PDF

Table 1. Regional stakeholders

Regional organisations	
OAS	
CICTE	The Inter-American Committee against Terrorism (CICTE) is the responsible organ for the cybersecurity programme on capacity building. It falls under the Secretariat for Multidimensional Security (SMS).
CITEL	The Inter-American Telecommunication Commission (CITEL) develops standards to secure the architecture of the Internet.
REMJA	The Ministers of Justice or Attorneys General of the Americas (REMJA) are responsible for strengthening inter-American cooperation against cybercrime.
IACHR	The Inter-American Commission on Human Rights (IACHR) monitors human rights violations online.
CSIRTsAmericas	The Computer Incident Response Teams for the Americas exchange information on cyber threats and incidents.
Committee on Hemispheric Security	The Committee on Hemispheric Security makes recommendations to the Permanent Council of the OAS and created the first Cyber Confidence Building Measure.
Inter-American Defense Board	The Inter-American Defense Board is responsible for cyberdefence coordination within the OAS.
Pacific Alliance	
GAD	The Digital Agenda Group (GAD) coordinates the Pacific Alliance's digital economy efforts.
MERCOSUR	
RAPRASIT	The meeting of authorities on information security and privacy and technological infrastructure (RAPRASIT) proposes common policies and initiatives relating to cybersecurity to MERCOSUR.
CEPAL	
eLAC	The United Nations Economic Commission for Latin America and the Caribbean (ECLAC, or as it's known in Spanish, CEPAL) creates digital agenda strategies for the information society eLAC.
CARICOM	
IMPACS	The Caribbean Implementation Agency for Crime and Security (IMPACS) is the coordination lead for the Caribbean Community's (CARICOM) Cyber Security and Cybercrime Action Plan.
CELAC	The Community of Latin American and Caribbean States (CELAC) is a political forum that consolidates Latin American positions in international forums
UNASUR ➔ PROSUR	The Union of South American Nations (UNASUR) was a regional organisation discussing cooperation on matters of regional security. It had a working group on cybersecurity and disintegrated in 2019. The Forum for the Progress and Development of South America (PROSUR) was created in 2019 to replace the dismantled UNASUR.
Ibero-American Cyber Defense Forum	The defence forum, composed of eight Latin American nations, Spain, and Portugal, discusses cyberdefence efforts and organises exercises.

Civil society actors with a focus on privacy, data protection, Internet governance, and content control are welcomed to participate in the OAS meetings on cybersecurity - which are held in the CICTE commission - as long as they receive the approval of hosting countries.[38] Civil society has a strong presence in Latin America through a loosely organised network of national organisations. On a national level, digital rights activists regularly face opposition by governments. There have been reports of espionage and hacking of civil society actors. For example, it was exposed in 2017 and 2018 that the Mexican government infected human rights defenders' and journalists' devices with spyware and refused international monitoring on its use of spyware.[39] Despite these barriers of trust, civil society is adamant about securing a place at the table due to most states' recent authoritarian histories. Notably, in Paraguay and Colombia, non-governmental experts from civil society and academia have reportedly played a role in creating a national cybersecurity strategy and regulations.[40] In Mexico, civil society was involved in the drafting of the national strategy, despite the aforementioned tense relationship with those stakeholders.[41] The level of participation was not, however, seen as sufficient by non-state actors, who perceived it as a legitimisation effort by the Mexican government.[42] States that have invited civil society into their policymaking discussions have added certain protections of human rights in the digital transformation to their national strategies.[43] Since civil society remains sceptical of the actual implementation of such safeguards, it acts as a watchdog for countries in the region.[44]

Table 2. Non-state stakeholder groups

National organisation	There are several national digital rights organisations that cooperate in the region. The most active are: Derechos Digitales (Chile), Asociación por los Derechos Civiles (ADC) (Argentina), Fundacion Capa 8 (Argentina), Karisma (Colombia), TEDIC (Mexico), Red en Defensa de los Derechos Digitales (R3D) (Mexico), Hiperderecho (Peru), ITS Rio (Brazil), Igarapé (Brazil), Fundación Getulio Vargas (FGV) (Brazil), IPANDETEC (Panama)…

[38] Sequera, Maricarmen; Toledo, Amalia & Ucciferri, Leandro (2018) 'Derechos Humanos y Seguridad Digital: Una Pareja Perfecta. El rol de organizaciones multilaterales en la agenda latinoamericana de seguridad digital, El caso de la OEA' TEDIC, la Asociación por los Derechos Civiles (ADC), Fundación Karisma https://www.tedic.org/wp-content/uploads/2018/06/DDHH-y-Seguridad-Digital-2-FINAL.pdf

[39] Privacy International (2019) 'State of Privacy Mexico' https://privacyinternational.org/state-privacy/1006/state-privacy-mexico

[40] Sequera, Maricarmen; Toledo, Amalia & Ucciferri, Leandro (2018) "Derechos Humanos y Seguridad Digital: Una Pareja Perfecta. El rol de organizaciones multilaterales en la agenda latinoamericana de seguridad digital, El caso de la OEA" TEDIC, la Asociación por los Derechos Civiles (ADC), Fundación Karisma https://www.tedic.org/wp-content/uploads/2018/06/DDHH-y-Seguridad-Digital-2-FINAL.pdf

[41] OAS & Presidency of the Republic of Mexico (2017) 'Hacia una Estrategia Nacional de Ciberseguridad. Consolidación de las Consultas a Actores Nacionales.'https://www.sites.oas.org/cyber/Documents/Mexico%20-%20Consolidacion%20de%20Consultas%20Documento%20ENCS%20(1).pdf

[42] "Sociedad civil al margen del diseño de la estrategia nacional de ciberseguridad https://sontusdatos.org/2017/09/22/sociedad_civil_margen_estrategia_nacional_ciberseguridad/

[43] See for example Colombia's National Digital Security Policy (2016) CONPES No. 3854. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf and Paraguay's national cybersecurity plan (2017) 'challenges, roles and commitments'. Decree 7052/2017 https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

[44] Sequera, Maricarmen; Toledo, Amalia & Ucciferri, Leandro (2018) "Derechos Humanos y Seguridad Digital: Una Pareja Perfecta. El rol de organizaciones multilaterales en la agenda latinoamericana de seguridad digital, El caso de la OEA" TEDIC, la Asociación por los Derechos Civiles (ADC), Fundación Karisma https://www.tedic.org/wp-content/uploads/2018/06/DDHH-y-Seguridad-Digital-2-FINAL.pdf

Technical community	
LACNIC	The Latin American and Caribbean Internet Addresses Registry (LACNIC) is the main organisation responsible for governance of Internet number resources in Latin America and does advocacy work for social inclusion in the Internet.
LAC-IGF	The Latin America and Caribbean Internet Governance Forum is the regional grouping of all local IGF groups in the region and gathers expertise to discuss Internet governance.
ISOC-LAC	The Internet Society for Latin America is the regional chapter of the Internet Society. It has a regional focus on helping the improvement of access, capacity development, and SDG implementation.
RedCLARA	The Latin American Cooperation of Advanced Networks (RedCLARA) gathers the technical academic research community and has been instrumental in creating the EllaLink submarine cable connecting Latin America with Europe.
FIRST	The International Forum of Incident Responders (FIRST) is a worldwide organisation for CSIRTS. It signed an agreement with the OAS to cooperate on incident response training.
Private sector	
CAF	The Development Bank of Latin America (CAF) plays a big part in implementing the digital economy initiatives and has done research on how a digital market could be modelled after European example.
IDB	The Inter-American Bank of Development (IDB) has supported the OAS in researching cyber maturity in the region.
REGULATEL	REGULATEL gathers all telecom regulators in Latin America and is instrumental in the creation of a digital regional market.
ASIET	The Inter-American Association of Telecommunication Enterprises is a private sector network of telecom industries that regularly engages in discussions with the Pacific Alliance and MERCOSUR.
Multinational businesses	Several companies work with the OAS on trainings, providing technical reviews of policies and creating analysis reports, such as Microsoft, Symantec, Trend Micro, Cisco, Citi Foundation, and Usuaria.
CISCO	OAS announced the launch of a cybersecurity Innovation Council in 2019 with Cisco.

3. Policy issues, priorities, and actions

3.1. Cooperating on resilience

Joint efforts to build resilience have been mostly coordinated through the OAS. The 2004 "Inter-American Integral Strategy to Combat Threats to Cyber Security" provided a mandate to the OAS to assist member states in the development of their cybersecurity capabilities.[45] The OAS institutions involved in this strategy were the Ministers of Justice or Attorneys General of the Americas (REMJA), the Inter-American Telecommunication Commission (CITEL), and the Inter-American Committee against

[45] Organization of American States (OAS) (2004) 'Adoption of a comprehensive inter-American strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity'

Terrorism (CICTE). CITEL was given the task of improving the security and confidentiality of the architecture of the Internet. This involved adapting national and regional telecom organisations to any international standard or practice without reducing the effectiveness of the entire network. Since then, it has incorporated digital security as one of the strategic objectives.[46] REMJA strengthens inter-American cooperation against cybercrime, which is discussed in 3.2. CICTE created a specific "cybersecurity programme" for the region.[47] 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. The OAS' 2004 strategy built a clear foundation for cybersecurity in the region and was updated in 2012 with the CICTE declaration on "Strengthening Cyber Security in the Americas".[48] This underscored the need for a hemispheric watch-and-warning network of Computer Security Incident Response Teams (CSIRTs) and pushed almost every member state to have a national CSIRT. These CSIRTs started cooperating through CSIRTAmericas.org in 2016.[49] CICTE adopted one more declaration in 2015 on "the Protection of Critical Infrastructure from Emerging Threats".[50] This expanded the cybersecurity programme with a broader technical assistance mandate, allowing the cybersecurity programme to create assistance projects for risk management on critical infrastructure in the region. The cybersecurity programme has become the central coordination hub for cybersecurity in the region. It also shares knowledge through regular white papers and capability surveys of the region.[51] Some civil society organisations question whether the perceived progress in the region has actually translated into an actual capacity to tackle cybersecurity issues, given that the OAS surveys are filled in by public officials.[52]

This observation also highlights one of the bottlenecks in the OAS programme; the ambitions for the region are highly dependent on national authorities' willingness to improve resilience. As stated in the introduction, progress has been slow since the 2004 cybersecurity strategy but seems to be picking up speed. Countries that had a mature national cybersecurity strategy in 2020 include Mexico, Trinidad and Tobago, the Dominican Republic, Jamaica, Costa Rica, Panama, Colombia, Brazil, Paraguay, Guatemala, Chile, and recently Argentina.[53] Most Latin American countries are in the process of developing a national cybersecurity strategy and currently have an action plan or guidelines for cybersecurity. Those willing to cooperate with the OAS have the possibility to request assistance through the cybersecurity

[46] Inter-American Telecommunication Commission (CITEL) 'Annual Report 2008, https://bit.ly/2G7CyKs; Annual Report 2011, https://bit.ly/2rAq7S3, Annual report 2015, https://bit.ly/2K8RRVC

[47] Organization of American States (OAS) 'Cybersecurity' https://www.sites.oas.org/cyber/en/pages/default.aspx

[48] Organization of American States (OAS) (2012) 'Declaration on Strengthening Cyber Security in the Americas' Inter-American Committee Against Terrorism (CICTE) https://www.oas.org/en/sms/cicte/Documents/Declarations/DEC_1%20rev_1_DECLARATION_CICTE00749E04.pdf

[49] Organization of American States (OAS) 'Cybersecurity' last accessed 04/07/2019 https://www.sites.oas.org/cyber/en/pages/default.aspx

[50] Organization of American States (OAS) (2015) 'Declaration on Protection of Critical Infrastructure from Emerging Threats' Inter-American Committee Against Terrorism (CICTE) https://www.oas.org/en/sms/cicte/Documents/Declarations/DEC_1%20rev_1_DECLARATION_CICTE00749E04.pdf

[51] Organization of American States (OAS) (2015) 'OAS Cybersecurity Initiative' presentation prepared for the Global Forum on Cyber Expertise (GFCE) https://www.sites.oas.org/cyber/Documents/2015%20OAS%20Cybersecurity%20Initiative.PDF

[52] Sequera, Maricarmen; Toledo, Amalia & Ucciferri, Leandro (2018) "Derechos Humanos y Seguridad Digital: Una Pareja Perfecta. El rol de organizaciones multilaterales en la agenda latinoamericana de seguridad digital, El caso de la OEA" TEDIC, la Asociación por los Derechos Civiles (ADC), Fundación Karisma https://www.tedic.org/wp-content/uploads/2018/06/DDHH-y-Seguridad-Digital-2-FINAL.pdf

[53] Organisation of American States "Cybersecurity Program" last accessed 12/02/2020 http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

programme. So far, Colombia, Paraguay, Mexico, Panama, Costa Rica, Trinidad and Tobago, Suriname, and Jamaica seem to have made use of these services.[54]

While the Caribbean does not receive a lot of attention in this paper, it is worth noting that the small and developing island states of the Caribbean have been struggling to navigate the various cyber capacity building efforts that are offered internationally. For this purpose, the OAS, the Commonwealth, the Caribbean Telecommunications Union, and CARICOM's Implementation Agency for Crime and Security (CARICOM IMPACS) elaborated a CARICOM Cyber Security and Cybercrime Action Plan in 2016. This main focus of the action plan has been to strategically coordinate efforts of these organisations for the Caribbean.[55]

3.2. Fight against cybercrime

The numbers in this paper's introduction show that cybercrime poses a significant threat for Latin America. Latin American states used to wrestle with a shortage of trained cybercrime law enforcement agents, but major efforts have been made in recent years to build capacity, mostly in cooperation with Interpol. The Interpol project Cyber Americas II, funded by the Canadian government, runs in all Latin American states and the Caribbean to build police capacities. It also established a working group on cybercrime for heads of units.[56]

On the judicial side, the OAS plays a significant role for prosecutors in the fight against cybercrime. The group of Ministers of Justice or Attorneys General of the Americas (REMJA) has strengthened mechanisms for information exchange and cooperation between states, the private sector and technology companies, and international instances. Following up on their commitments in the 2004 cybersecurity strategy, REMJA also organises workshops for police and judicial authorities to increase their capacity and to pursue and prosecute computer crimes.[57] The 2004 strategy was not even the starting point for REMJA; they had already established a working group on cybercrime in 1999 and created a portal to streamline cooperation.[58]

REMJA has recommended for more than 10 years that OAS member states use the Budapest Convention on Cybercrime as a guideline.[59] Argentina, Chile, Costa Rica, Panama, Paraguay, and Peru are currently part of the Budapest convention, with Colombia and Mexico as observer countries.[60] Most of these countries have adjusted their criminal code to be in line with the Budapest Convention, while other Latin

[54] Sequera, Maricarmen; Toledo, Amalia & Ucciferri, Leandro (2018) 'Derechos Humanos y Seguridad Digital: Una Pareja Perfecta. El rol de organizaciones multilaterales en la agenda latinoamericana de seguridad digital, El caso de la OEA' TEDIC, la Asociación por los Derechos Civiles (ADC), Fundación Karisma https://www.tedic.org/wp-content/uploads/2018/06/DDHH-y-Seguridad-Digital-2-FINAL.pdf

[55] CARICOM Caribbean Community (2016) 'CARICOM Cyber Security and Cybercrime Action Plan' https://www.caricomimpacs.org/Portals/0/Project%20Documents/CCSAP.pdf

[56] Interpol (2018) "Interpol Project to Combat Cybercrime in the Americas" https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2018/INTERPOL-project-to-combat-cybercrime-in-the-Americas

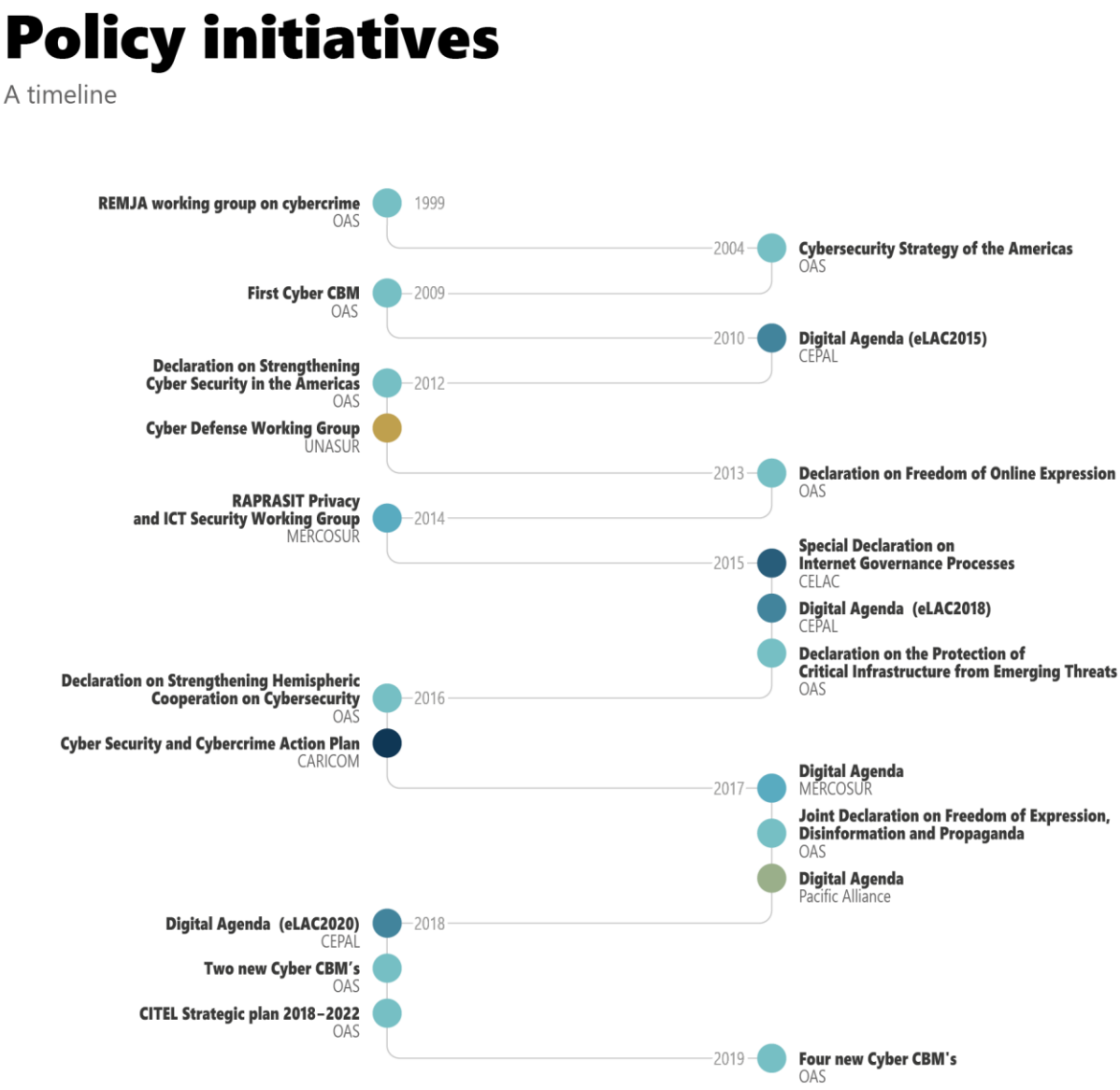
[57] Organization of American States (OAS) (2016) 'Cybercrime: 90 Billion reasons to prosecute it' E-063/16 http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-063/16

[58] Organization of American States (1999) 'Conclusions And Recommendations Of The Second Meeting Of Ministers Of Justice Or Of Ministers Or Attorney General Of The Americas' http://www.oas.org/juridico/english/cybII_CR.doc

[59] Organization of American States (OAS) Inter-American Development Bank (IDB) (2016) 'cybersecurity: are we prepared in Latin America and the Caribbean'

[60] Council of Europe' Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY' (last accessed on 04/07/2019) https://www.coe.int/en/web/cybercrime/parties-observers

American states use the convention as a baseline in the development of cybercrime legislation. Brazil also requested to join the Budapest Convention in 2019.[61] This was a surprising move as Brazil has repeatedly expressed scepticism over the Budapest Convention, preferring the creation of a multilateral framework on cybercrime at the UN instead.[62]



[61] Council of Europe (2019) 'Budapest Convention: Brazil invited to accede" https://www.coe.int/en/web/cybercrime/-/budapest-convention-brazil-invited-to-accede

[62] United Nations Commission on Crime Prevention and Criminal Justice (2015) 'Non-Paper submitted by Brazil reflecting its views on the issue of cybercrime' E/CN.15/2015/CRP.5 https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_24/ECN152015_CRP5_e_V1503408.pdf

Almost all member states have increased their law enforcement efforts domestically and have updated national legislation to combat cybercrime. The successful prosecution of cybercrimes in the region, however, is still hampered by the absence in most states of a formal mechanism for reporting cyber incidents. The exceptions are Colombia and Mexico, where notifying the authorities is required, and Peru, where notifying the subjects of a data breach is required.[63] With no legislation in place in the rest of the region to force organisations to disclose if they have been a victim of cyberattacks, a legal handicap when it comes to battling cybercrime remains.

3.3. Building confidence

The OAS has been successful in developing confidence building measures (CBM) for the region. The OAS was the first region in the world to mention confidence building in cyberspace. The first reference to a cyber CBM was contained in the 2009 declaration by the OAS committee on hemispheric security.[64] In a 2016 declaration on strengthening Hemispheric Cooperation and Developments in Cybersecurity and Fighting Terrorism, member states committed to creating cyber-specific confidence building measures to increase stability in cyberspace.[65] The 2016 declaration established a working group in CICTE. In 2018, the cyber CBMs working group agreed on a first set of voluntary cyber confidence building measures. These initial CBMs would encourage member states to share information on national cybersecurity policies and would also identify a national point of contact at the policy level (see Table 3.3 below).[66] The second working group in 2019 proposed four more CBMs, primarily focused on cyber diplomacy and building the capacities of foreign ministries and diplomats.[67] The implementation of these CBMs is followed up by the OAS secretariat.

Table 3. Cyber-related Confidence-Building Measures

	Confidence building measures
2009 Committee on Hemispheric Security	**#1** Member states exchange information related to adopting and adapting provisions under domestic laws that govern processes for obtaining data and information. They exchange experiences involving government, service providers, end users, and others regarding prevention, management of, and protection against **cyber threats** with a view to sustained mutual cooperation. They do so to prevent, address, and **investigate criminal activities** that threaten security and to ensure an open, interoperable, secure, and reliable Internet. At the same time, they respect obligations and commitments under international law and international human rights law, in particular.
2018 Working Group on Cooperation and Confidence Building Measures in Cyberspace	**#2** Provide information on national cybersecurity policies, such as national strategies, white papers, legal frameworks, and other documents that each member state considers relevant.

[63] Iliopulos, Aris (2017)"Latin America has a long way to go on cyber-security" The Economist

[64] Organization of American States (OAS) 'Consolidated List of Confidence and Security Building Measures for Reporting according to OAS Resolutions' (Approved at the meeting of January 15, 2009) CP/CSH-1043/08 rev. 1

[65] Organization of American States (OAS) (2016) 'Declaration on Strengthening Hemispheric Cooperation and Development in Cybersecurity and Fighting Terrorism in The Americas' Inter-American Committee Against Terrorism (CICTE) http://www.oas.org/en/sms/cicte/Documents/2016/Declaration/CICTE%20DEC%201%20DECLARATION%20ENGLISH%20CICTE01037E04.pdf

[66] Organization of American States (OAS) (2018) 'Resolution on Regional Confidence Building Measures (CBM's) to promote cooperation and trust in cyberspace' OEA/Ser.L/X.2.18

[67] Organization of American States (OAS) (2019) 'Regional Confidence-Building Measures (CBMs) to Promote Cooperation and Trust in Cyberspace' Inter-American Committee Against Terrorism (CICTE) CICTE/RES. 1/19 http://scm.oas.org/doc_public/ENGLISH/HIST_19/CICTE01297E03.doc

	#3 Identify a national point of contact at the policy level able to discuss the implications of hemispheric cyber threats. The work of these national points of contact may be distinct from the ongoing work of law enforcement and other technical experts in combating cybercrime and responding to cyber incidents of concern, while at the same time supplementing them. The information on these national points of contacts will be updated annually, or as frequently as needed, and shared among the national point of contacts in a transparent and readily accessible format.
2019 Working Group on Cooperation and Confidence Building Measures in Cyberspace	**#4** To designate points of contact, in the event that none exist, within foreign ministries, with the purpose of facilitating work on international cooperation and dialogue in cybersecurity and cyberspace. **#5** Develop and strengthen capacity building through activities such as seminars, conferences, and workshops, among others, for public officials and the private sector in cyber diplomacy. **#6** To foster the inclusion of cybersecurity and cyberspace subjects into training courses for diplomats and officials of foreign ministries and other government agencies. **#7** To foster cooperation and exchange of best practices on cyber diplomacy, cybersecurity, and cyberspace, through, for example, the establishment of working groups, other dialogue mechanisms, and the signing of agreements among states.

The latest CBM working group in 2019 focused on foreign ministries. This was novel compared to CBMs created in other regional groups, such as the OSCE. It was, however, not surprising to be initiated under the auspices of the OAS. The national points of contact for the OAS are usually diplomatic missions, which are important stakeholders in the coordination of the cybersecurity programme. Strengthening cybersecurity expertise and appointing a cyber coordinator thus facilitates cooperation between OAS member states, especially since most countries have fragmented digital policy responsibilities over several ministries. This new set of CBMs also facilitates international cooperation and creates a baseline expertise level for engagement in multilateral fora. This is particularly useful when cybersecurity is being discussed at the United Nations. In the new UNGGE mandate, there is also a role for regional organisations and the OAS is appointed as the regional representative for Latin America. The first consultation of the UNGGE chair took place in Washington in August 2019. During this consultation, it was noted that the OAS working group on CBMs enhances cooperation and provides an excellent platform to implement confidence building measures.[68]

3.4. Protecting democracy

Privacy and freedom of online expression is an established policy issue for the region that is increasingly becoming part of cybersecurity discussions. The OAS consolidated its stance on online freedoms by co-

[68] United Nations Office of Disarmament Affairs (2019) 'Collated Summaries of the Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf

signing a declaration on Freedom of Expression and Access to Information in 2011 with other regional organisations and the UN special rapporteur.[69] The OAS' Inter-American Commission on Human Rights (IACHR) reiterated this stance for online expression in 2013. In this declaration, the IACHR recommended avoiding a broad view of the concept of "cybersecurity" that could lead to the criminalisation of the use of the Internet.[70] To deal with a changing information space, in 2017, the OAS adopted a joint declaration on freedom of expression and "fake news", disinformation and propaganda with other regional organisations and the UN special rapporteur.[71] This declaration permits restrictions on freedom of expression as long as they serve legitimate interests recognised under international law.

Civil society organisations, however, warn against worrying trends in surveillance technology.[72] Governments seem to be falling in the "technological solutionism" trap to fix all societal issues with digital technology. Their intentions are not necessarily malicious. There appears to be a lack of critical thinking from governments in implementing innovative technologies that do not comply with human rights standards.[73]

Latin American states have been vocal about protecting the freedom of online expression and human rights on the Internet in multilateral fora such as the UN Open-Ended Working Group.[74] The implementation of those values and obligations on a domestic level, however, is not very promising. Freedom House's "Freedom of the Net" index shows several Latin American countries dropping in online freedoms, like Brazil,[75] Colombia,[76] and Venezuela,[77] and some slightly improving but still fitting the category of only "partly free", like Mexico[78] and Ecuador.[79] Countries in the region also appear to be struggling to cope with increasing information disorder, whereby social media is flooded with disinformation, as became apparent in the Brazilian elections.[80] Institutional protection is, however,

[69] Organisation of American States (OAS) UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, and the special rapporteur of the African Commission on Human Rights and People's Rights (ACHPR) 'Joint declaration on freedom of expression and the Internet' https://www.oas.org/en/iachr/expression/showarticle.asp?artID=848

[70] Organisation of American States (OAS) (2013) "Freedom of Expression and the Internet" Inter-American Commission on Human Rights OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13

[71] UNHR, OAS, OSCE, ACHPR (2017) 'Joint Declaration On Freedom Of Expression And "Fake News"Disinformation And Propaganda' https://www.law-democracy.org/live/wp-content/uploads/2017/03/mandates.decl_.2017.fake-news.pdf

[72] Pérez Acha, G. (2016)'Hacking Team: The rise of surveillance software in Latin America' Derechos Digitales https://www.derechosdigitales.org/9880/el-auge-del-software-de-vigilancia-en-america-latina/

[73] Sequera, Maricarmen; Toledo, Amalia & Ucciferri, Leandro (2018) "Derechos Humanos y Seguridad Digital: Una Pareja Perfecta. Aportes de la sociedad civil hacia políticas nacionales de seguridad digital que respeten y protejan los derechos humanos' TEDIC, la Asociación por los Derechos Civiles (ADC), Fundación Karisma https://www.tedic.org/wp-content/uploads/2018/12/InformeCiberseguridadParte1.pdf

[74] Among others, Colombia, Argentina, Costa Rica, Brazil, Mexico mentioned the protection of human rights in their statements at the 1st session of the Open-ended Working Group (OEWG) on 'Developments in the field of information and communications technology in the context of international security' in 2019

[75] Freedom House (2019) 'Freedom on the Net 2019: Brazil' https://www.freedomonthenet.org/country/brazil/freedom-on-the-net/2019

[76] Freedom House (2019) 'Freedom on the Net 2019: Colombia' https://www.freedomonthenet.org/country/colombia/freedom-on-the-net/2019

[77] Freedom House (2019) 'Freedom on the Net 2019: Venezuela' https://www.freedomonthenet.org/country/venezuela/freedom-on-the-net/2019

[78] Freedom House (2019) 'Freedom on the Net 2019: Mexico' https://www.freedomonthenet.org/country/mexico/freedom-on-the-net/2019

[79]Freedom House (2019) 'Freedom on the Net 2019: Ecuador' https://www.freedomonthenet.org/country/ecuador/freedom-on-the-net/2019

[80] Wardle, Claire (2019) 'What 100,000 WhatsApp messages reveal about misinformation in Brazil' First Draft https://firstdraftnews.org/latest/what-100000-whatsapp-messages-reveal-about-misinformation-in-brazil/

provided by the Inter-American Commission on Human Rights, which can bring violations before the Inter-American Court of Human Rights. The commission regularly monitors the impact of the Internet on human rights in the region and it has created a recommendation report with standards for a free, open, and inclusive Internet.[81] Civil society recommends a deeper integration of this commission into other bodies of the OAS that are involved in cybersecurity.[82]

3.5. Boosting the digital economy

Boosting the digital economy is a policy issue that can only be accomplished by providing cybersecurity. The digital economy and in general "connectivity" are definitely a priority for the region. This is evident from how ICTs have been formally recognised by the OAS' general secretariat as an essential tool for development in Latin American countries. This decision spurred the CITEL to create community networks in rural areas with the Internet Society in 2018 in order to provide more connectivity in remote areas of the Americas.[83] Harmonisation of the regulations and standards has been a priority of the digital agendas of the Pacific Alliance, MERCOSUR, and UNASUR. Much of their work is gathered in the United Nations Economic Commission for Latin America and the Caribbean (CEPAL)'s digital agenda roadmaps for the region, the last being the eLAC2020 digital agenda.[84] CEPAL also facilitated talks about the "Mercado Digital Regional", for which a roadmap is still being developed, with the support of the European Union's Digital Single Market expertise. Currently, regional organisations are mostly focusing on smaller building blocks to facilitate a regional digital market, such as consumer protection standards. As the regional organisations are starting to understand that digital markets are vulnerable, the Pacific Alliance and MERCOSUR have now included cybersecurity measures in their digital agendas. The Pacific Alliance has defined the development of national strategies and cooperation between CERT's as priorities in the roadmap of its digital agenda in 2018.[85] MERCOSUR's Digital Agenda Group included security and trust in the digital sphere as a priority for action in 2017. [86] While the digital economy blooms, the belated development of the digital market can be seen as an advantage. Security-by-design can now be part of the digital integration process, where connections are secured from the start.

Under UNASUR, a plan was also launched to build and connect the fibre optic networks between the countries in the region, with the goal of making the continent's telecommunications more secure. This effort was mostly incentivised by the 2013 revelations of the US' surveillance operations in the continent. UNASUR pledged $1.5 million in 2015 to let the development bank of Latin America (CAF) study the

[81] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (2017) 'Standards for a Free, Open and Inclusive Internet' http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf

[82] Sequera, Maricarmen; Toledo, Amalia & Ucciferri, Leandro (2018) "Derechos Humanos y Seguridad Digital: Una Pareja Perfecta. Aportes de la sociedad civil hacia políticas nacionales de seguridad digital que respeten y protejan los derechos humanos' TEDIC, la Asociación por los Derechos Civiles (ADC), Fundación Karisma https://www.tedic.org/wp-content/uploads/2018/12/InformeCiberseguridadParte1.pdf

[83] Internet Society (2018) 'Internet Society and the OAS through CITEL sign an agreement to bring the Internet closer to rural areas of the Americas' https://www.Internetsociety.org/news/press-releases/2018/Internet-society-and-the-oas-through-citel-sign-an-agreement-to-bring-the-Internet-closer-to-rural-areas-of-the-americas/

[84] CEPAL (2018) 'Follow-Up Mechanism for the Digital Agenda for Latin America and the Caribbean (eLAC2020) for the Period 2018-2020' LC/CMSI.6/3/Rev.2 https://repositorio.cepal.org/bitstream/handle/11362/43329/S1800464_en.pdf?sequence=4&isAllowed=y

[85] Palacio, Ana Maria (2017) 'Roadmap for the Pacific Alliance's Digital Agenda' Pacific Alliance Blog http://pacificallianceblog.com/roadmap-pacific-alliances-digital-agenda/

[86] MERCOSUR (2017) 'Agenda Digital del MERCOSUR' CMC/DEC 27/17

feasibility of a "South American Connectivity Network for Integration".[87] UNASUR heads of states mentioned these efforts in the 2015 UN General Assembly, saying they would make sure the national fibre optic networks would be secure.[88] Given the implosion of UNASUR, it is unclear who will be coordinating the implementation of this project. Regional connectivity will however also be improved under the BELLA project that is building an underwater fibre optic cable between Latin America and Europe, as the cable will also be extended throughout Latin America.[89]

3.6. Military cyber presence

A policy issue that is growing in relevance in Latin America is military cyberdefence. UNASUR, which was created in 2008 to promote a security cooperation agenda, pioneered this issue with a cyberdefence working group in 2012.[90] This initiative came from the countries who initially placed their national cybersecurity coordination in the Ministry of Defence, like Brazil, Colombia, and Argentina. As mentioned before, most countries suspended their membership to UNASUR by the end of 2018, leaving the organisation dead in the water.[91] The defence cooperation is still alive in different fora. Since 2016, there has been an Ibero-American Cyber Defence Forum composed of eight Latin American nations,[92] plus Spain and Portugal. The forum organised its first cyberdefence exercise in 2017, led by Brazil. The 10 countries agreed in a 2019 meeting in Brazil to jointly implement MISP, the Malware Information Sharing tool used by NATO members.[93] The Inter-American Defence board at the OAS also organised a first cyberdefence conference in the Western Hemisphere in 2019 in Colombia.[94] The defence ministers of Brazil and Argentina have been cooperating on cyberdefence for a lot longer, and had already signed a Joint Declaration in 2011 that included cyberdefence.[95] The two states are known to have cooperated on information exchange, research, training, and exercises through a working group in cyberdefence between 2014 and 2017.[96] The US Cyber Command and the US government have also inked deals with

[87] UNASUR (2015) 'Conectividad y fibra óptica es otro de los objetivos de UNASUR' https://web.archive.org/web/20190704091712/http://www.unasursg.org/node/152
CAF (2015) 'USD 1,5 millones para el desarrollo de la red de banda ancha suramericana' Development Bank of Latin America https://www.caf.com/es/actualidad/noticias/2015/02/usd-1-5-millones-para-el-desarrollo-de-la-red-de-banda-ancha-suramericana/

[88] UNGA (2015) 'Potential Security Impacts of Cyberspace Misuse Considered in First Committee, as Speakers Warn of Arms Race, Emergence of New Theatre of Warfare' 70th UNGA session GA/DIS/3537 https://www.un.org/press/en/2015/gadis3537.doc.htm

[89] European Commission (2018) 'BELLA: A new digital data highway between Europe and Latin America' Digital Single Market https://ec.europa.eu/digital-single-market/en/news/bella-new-digital-data-highway-between-europe-and-Latin America

[90] Martins, Paula (ed) (2017) 'Brazil: Investigating policy initiatives on cyber security and cyber-defence in South America' Article 19 https://www.article19.org/resources/brazil-new-report-analyses-brazils-policy-initiatives-cybersecurity-cyber-defence-south-america/

[91] Reuters (2018) 'Six South American nations suspend membership of anti-U.S. bloc' https://www.reuters.com/article/us-unasur-membership/six-south-american-nations-suspend-membership-of-anti-u-s-bloc-idUSKBN1HR2P6

[92] Members: Argentina, Chile, Colombia, Mexico, Paraguay, Peru, Uruguay, and Brazil

[93] Barreto, Andréa (2019) 'Brazil Promotes Cyberthreat Information Sharing' Dialogo https://dialogo-americas.com/en/articles/brazil-promotes-cyberthreat-information-sharing

[94] Comando General Fuerzas Militares de Colombia (2019) 'Colombia sede de la 'I Conferencia de Ciberdefensa: Hemisferio Occidental'' https://www.cgfm.mil.co/en/node/4292

[95] Gustavo Diniz, Robert Muggah and Misha Glenny, "Deconstructing Cyber Security in Brazil: Threats and Responses", Igarape Institute, 2014, p.7, available at https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf.

[96] Martins, Paula (ed) (2017) 'Brazil: Investigating policy initiatives on cyber security and cyber-defence in South America' Article 19 https://www.article19.org/resources/brazil-new-report-analyses-brazils-policy-initiatives-cybersecurity-cyber-defence-south-america/

Chile,[97] Argentina,[98] and Colombia[99] to cooperate in cyberspace and share information, and Colombia also became the first South American partner of NATO in 2017.[100]

4. Regional approaches to cyber diplomacy and resilience

Cyber diplomacy, the use of diplomatic means to create stability in cyberspace, remains a new domain of international engagement. Latin American states have participated in these debates in the last few years and formed a consensus on several topics, but they have not formed a comprehensive cyber diplomacy strategy for the region or decided to what benefit it could be used. The discussions in the OAS' confidence building working group have the potential to align national interests among OAS members and form a regional cyber diplomacy strategy to build a secure and rights-based global cyberspace. Mexico seems intent to use CELAC to unify positions more at multilateral fora and to speak with one voice. Given the composition of the group compared to the OAS, this group might have a different perception on international state behaviour in cyberspace. It might also provide CELAC member states with a stronger brokering position to negotiate with one of the more dominant players in cyberspace, the United States. The following sections provide an overview of national and regional positions on the cyberspace issues that are being hotly debated at multilateral fora, specifically the United Nations.

4.1. The international law and norms debate

Opposition to international surveillance was one of the first issues in which Latin American states found each other in regional consensus. They jointly iterated in 2013 at the UNGA, through CELAC and UNASUR, that the American surveillance operations were a violation of human, civil, and political rights and breached sovereignty and international law.[101] On the forefront of this bloc were Cuba, Ecuador, Venezuela, and Brazil. Brazil consequently became more sceptical towards the US' influence over ICANN and joined the EU in advocating for more inclusiveness and accountability of the global Internet governance model.[102]

---

[97] VOANews (2018) 'US, Chile Agree to Cooperate on Cyber Security' https://www.voanews.com/americas/us-chile-agree-cooperate-cyber-security

[98] US Embassy in Argentina (2017) 'United States and Argentina Strengthen Partnership on Cyber Policy' https://ar.usembassy.gov/united-states-argentina-strengthen-partnership-cyber-policy/

[99] Dialogo (2016) 'Cybersecurity Highlights First Ever United States-Colombia CCIB' https://dialogo-americas.com/articles/cybersecurity-highlights-first-ever-united-states-colombia-ccib/

[100] North Atlantic Treaty Organisation 'Relations with Colombia' last updated 06 December 2018 https://www.nato.int/cps/en/natohq/topics_143936.htm

[101] CELAC statement at the UNGA: United Nations General Assembly (2013) 'Statement By H.E. Mr. Bruno Rodriguez Parrilla, Minister For Foreign Affairs Of The Republic Of Cuba, On Behalf Of The Community Of Latin American And Caribbean States (CELAC) At The General Debate Of The Sixty Eighth Session Of The United Nations

UNASUR statement in the 1st committee: United Nations General Assembly First Committee (2013) debates agenda items 89 to 107 A/C.1/68/PV.20 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/537/73/PDF/N1353773.pdf?OpenElement

Brazil statement at the UNGA: United Nations General Assemblee (2013) "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" https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf

[102] Diniz, Gustavo ; Muggah, Robert and Glenny, Misha (2014) 'Deconstructing Cyber Security in Brazil: Threats and Responses", *I*garape Institute https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf.

Latin American countries have shared some positions on international stability in cyberspace, which is clear from the statements made at the United Nations, listed below in Table 4.1. On the matter of international law, they endorsed the UNGGE 2015 reports and, through CELAC and UNASUR statements at the UN 1st committee, agreed that international law is applicable to cyberspace. The need to draw up specific legally binding standards was once uttered at the UN by UNASUR in 2016, and repeated by Cuba, but did not reappear unanimously in the latest Open-ended Working Group (OEWG). Latin states like Ecuador, Argentina, Colombia, and Brazil endorsed the available body of international law and expressed the need for more views of how international law applies. Nine states have replied to the OAS' Inter-American Juridical Committee's questionnaire on international law as of March 2020. These states, Bolivia, Chile, Costa Rica, Ecuador, Guatemala, Guyana, Peru and Brazil, provided some insights in national perspectives on the application of international law to regulate state behavior in cyberspace. It was indicated by several states and concluded by the rapporteur that there is an unevenness in states' capacities to study the application of international law.[103] Mexico proposed the creation of a working group in the International Law Commission (ILC) at the Second Substantive Session of the OEWG. This could produce a study on the applicability of current international law in cyberspace, complementary to national positions.[104] There is consensus not to change the norms and principles that have previously been agreed on at the United Nations and focus on implementation as the CELAC and UNASUR statements in Table 4.1 show. The region has already started the process of norms implementation through the OAS, which used the three UNGGE reports as a basis for its working group on Cyber Confidence Building Measures in 2017.[105] Mexico proposed an implementation mechanism for cybernorms at the 1st session of the Open-ended Working Group.[106] 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. This proposition was endorsed by several other states in the region and warmly welcomed by civil society organisations.[107] In line with this proposal, civil society supported the development of a multi-stakeholder mechanism to review implementation of agreed norms, similar to the Universal Periodic Review process of the Human Rights Council.[108]

Using the United Nations as a venue for this peace and security in cyberspace dialogue is supported by several Latin American states as is clear from the statements on institutional dialogue (see Table 4.1). There have been requests to open up the process and allow greater involvement since 2015. It was therefore not surprising that most Latin countries voted for both the resolution that established another iteration of the UN Group of Governmental Experts and the resolution that established the new Open-ended Working Group. The latter would allow for a more inclusive process, according to most Latin states. It became clear in the 1st sessions of the OEWG that this inclusive process also grants a voice to

[103] Hollis, Duncan B. (2020) 'Improving transparency international law and state cyber operations: Fourth Report' *Inter-American Juridical Committee of the Organisation of American States*, CJI/doc. 603/20 rev.1 corr.1

[104] 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 can be found at https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/mexico-study-of-the-ilc-applicability-of-international-law-in-cyberspace.pdf

[105] Organisation of American States (OAS) (2017) 'Establishment of a working group on cooperation and confidence building measures in cyberspace', Inter-American Committee Against Terrorism (CICTE) CICTE/RES. 1/17

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

[107] See for example the ICT4Peace submission for a "States Cyber Peer Review Mechanism for state-conducted foreign cyber operations", which explicitly supports the proposal by the Mexican delegations https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/ict4p-peace-proposed-states-cyber-peer-review-3.pdf

[108] Association for Progressive Communications (2020) 'Civil Society Statement at the Second Substantive Session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security' https://www.apc.org/en/pubs/apc-statement-un-open-ended-working-group-international-cybersecurity

non-governmental stakeholders. Some Latin states, most notably Brazil, spoke out in the intersessional multi-stakeholder meeting in support of participation by non-state actors.

Four countries voted against the launch of a new UNGGE: Cuba, Bolivia, Nicaragua, and Venezuela. These have also not coincidentally been the states that have been vocal against the militarisation of cyberspace. From their previous statements made at the UN as seen in the table below, we can deduce that these states perceived the UNGGE as an organ that intends to legitimise a regulated use of cyber weapons. Venezuela's 2015 UN statement hints that it holds the United States accountable for this evolution, as it lists the cyber offensive capabilities of "one country in particular" to be responsible for a militarisation of cyberspace.

Unease about the use of offensive cyber capabilities is not restricted to these four countries. Statements were made by Latin American countries on behalf of UNASUR in 2015 and 2016, warning for the development of offensive cyber capabilities and proposing the adoption of a no-first-use standard for offensive operations. A few other states also warned against the weaponisation of ICT tools, including Peru and Brazil in the 2019 OEWG.

Table 4. Cyber-related statements at the United Nations

International law	
2013 UN 1st Committee UNASUR	States or non-state actors should not use information and communications technologies **in violation of international law or human rights law** or any principle of the peaceful relations between sovereign states or the privacy of citizens.
2015 UN 1st Committee UNASUR	**International law**, especially the Charter of the United Nations, **is applicable** and crucial to maintaining peace and stability and promoting open, secure, peaceful, and accessible information and communication technologies.
2016 UN 1st Committee UNASUR	The international community should consider the need to draw up **specific legally binding standards** to meet the challenges of the digital age.
2017 UNGGE national view Ecuador	Ecuador supports the efforts made to continue studying [...] the **way in which international law should be applied** to the use of information and communications technologies by states.
2018 UN 1st Committee Cuba	[The Open-ended Working Group] provides the only adequate multilateral negotiating process to adopt an **international legally binding cybersecurity instrument.**
2019 UNGGE national view Argentina	It is essential to **achieve consensus on how international law applies** to cyberspace, which requires **dialogue and transparency regarding the vision** of each state.
2019 UNGGE national view Colombia	The applicability of international law to cyber operations requires **further study** in order to ensure there are **no grey areas or differences in interpretation** regarding how it applies.
2019 UN OEWG 1st session Brazil	There is a need for **further clarification on how exactly international law applies to cyberspace**, including means of adopting specific rules, norms, and principles of a legally binding nature.
2019 UN OEWG 1st session Argentina	The cybersecurity agenda should be interlinked with the international legal framework applicable to the **protection and promotion of human rights.**
2019 UN OEWG 1st session Cuba	CBMs, transparency, and capacity building do not replace the **need for** a **legally binding instrument.**
Norms	
2015 UN 1st Committee CELAC	Support **reinforcing the international norms and principles** applicable to states in the area of information and telecommunications in the context of

	international security, **by promoting actions and strategies** aimed at strengthening cybersecurity and preventing cybercrime.
2016 UN 1st Committee UNASUR	Support a **strengthening of the international standards and principles** applicable to states in the field of information and telecommunications in the context of international security.
2018 UN 1st Committee CELAC	Encourage the **strengthening of international norms** for states in the field of information and telecommunications within the context of international security by **fostering actions and strategies** aimed at strengthening cybersecurity.

Institutional dialogue

2013 UN 1st Committee UNASUR	**Regular institutional dialogue under United Nations auspices should be strengthened** in order to build trust, transparency, and confidence.
2015 1st Committee UNASUR	Discussions on this subject would benefit from **greater involvement by developing countries**.
2018 UN 1st Committee Mexico	We should **build**, on the basis of the UNGGE findings, **new agreements** on **how to implement international law** and non-binding **norms** and principles on the responsible behaviour of states.
2018 UN 1st Committee Cuba	L.37" would create a group of governmental experts that would duplicate previous efforts and increase the regular budget of the United Nations.
2019 UNGGE national view Argentina	It is necessary to continue to work within the framework of the United Nations processes, such as the Group of Governmental Experts and the Open-ended Working Group. It is crucial to **develop mechanisms and instruments** that can quickly **adapt to the changes and new challenges** continuously generated by the rapid progress of technology.
2019 UN OEWG 1st session Brazil	The OEWG should **not focus on issues that can be left to other fora**, such as Internet governance.
2019 UN OEWG 1st session Mexico	Mexico proposes a **follow-up implementation mechanism**. There should be a **periodic presentation of national reports** regarding the implementation of rules, norms, and principles. It would serve as a **roadmap** on what the member states need to agree upon in the future.
2019 UN OEWG 1st session Cuba	Establish a **central mechanism** under the auspices of the United Nations for **verification among states** in order to mitigate any potential **misuse of attribution.**
2019 OEWG intersessional Brazil	The OEWG should consider the report of the High-level Panel on Digital Cooperation, as it explains how multilateralism should be **complemented by multi-stakeholderism**. Brazil suggested that non-state actors should also be included in the decisionmaking.

Offensive capabilities

2015 UNGA declaration UNASUR	Aware that the development of offensive capacities in cyberspace is part of military doctrines, the member states of UNASUR share a **growing concern about the vulnerability of their critical infrastructure** and the possible escalation of conflicts driven by cyberattacks.
2015 UN 1st Committee Venezuela	More than 40 states are developing **military cyber capacities**, at least 12 of them for offensive action within the framework of a cyber war. One country in particular occupies a privileged position in the development of a capacity for cyberattacks, with a cyber force of more than 6,200 people divided among 33 teams working on defence, espionage, and attack in cyberspace. If we consider that a general and large-scale cyberattack could disrupt a state's critical infrastructure, causing total collapse with an **incalculable human cost**, we should be **worried about the direction being taken in the debate over banning arms from cyberspace or militarising it.**
2016 UNGA declaration UNASUR	Member states of UNASUR propose the adoption of a **no-first-use standard** on offensive operations using information and telecommunications technology. In addition to **reducing the possibilities of an arms race**, the no-first-use rule would ensure that such technologies would not be used as tools of aggression.
2018 UN 1st Committee Cuba	Cuba rejects the militarisation of cyberspace, calling for the development of international norms to **put an end to the illegitimate of use of information and communications technology.**

2019 UN OEWG 1st session Brazil	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.
2019 UN OEWG 1st session Peru	Peru expressed concern that states are developing their ICT capacities towards **military ends**.
2019 UN OEWG 1st session Cuba	Attempts to make cyberspace a theatre of military operations must be rejected. It is not acceptable that we seek to draw an **equivalence between the misuse of ICTs** and the **concept of armed attacks in article 51** of the UN Charter.

4.2. Cybercrime

Discussions on stability in cyberspace have played out almost entirely in the UN's 1st committee on disarmament, but observers warn that discussions on cybercrime will also have a significant impact on the stability of a rights- and rules-based Internet.[109] This is the case for a new cybercrime resolution that is being discussed at the UN 3rd Committee, which could create a competing instrument with the Budapest Convention.[110] The Budapest Convention is regularly put forward as the potential global regulatory framework. The Budapest Convention is also the recommended framework for cooperation by the OAS and signatories include Argentina, Chile, Costa Rica, Panama, Paraguay, and Peru. States like Brazil that were not part of the Budapest negotiations have portrayed the Budapest Convention as biased and have sought to strengthen alternative multilateral institutions to address cybercrime. Brazil recurrently referred to the work of the open-ended intergovernmental expert group on cybercrime at UNODC to develop multilateral solutions.[111] In 2018, Brazil co-sponsored this new resolution in the UN 3rd Committee for the creation of a multilateral framework on cybercrime at the UN, advanced by Russia and China, and also co-sponsored by Venezuela, Cuba, and Nicaragua.[112] Several other Latin states voted in favour. This resolution raised some serious human rights concerns, as the vagueness of the resolution could open the door to criminalising online behaviour that is protected under international human rights law.[113] Brazil, however, revised its support when it decided to abstain from voting for this resolution in 2019. It even requested to accede to the Budapest Convention in 2019. A few others Latin states went from voting Yes to abstaining or voting No. This did not stop the resolution from getting approved, and it will establish a committee of experts to consider a new UN cybercrime treaty.[114] It is unclear how the region will engage in these discussions, as the voting pattern shows how the region is undecided over this initiative.

[109] Hakmeh, Joyce & Peters, Allison (2020) 'A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet' Council on Foreign Relations Net Politics blog https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-Internet

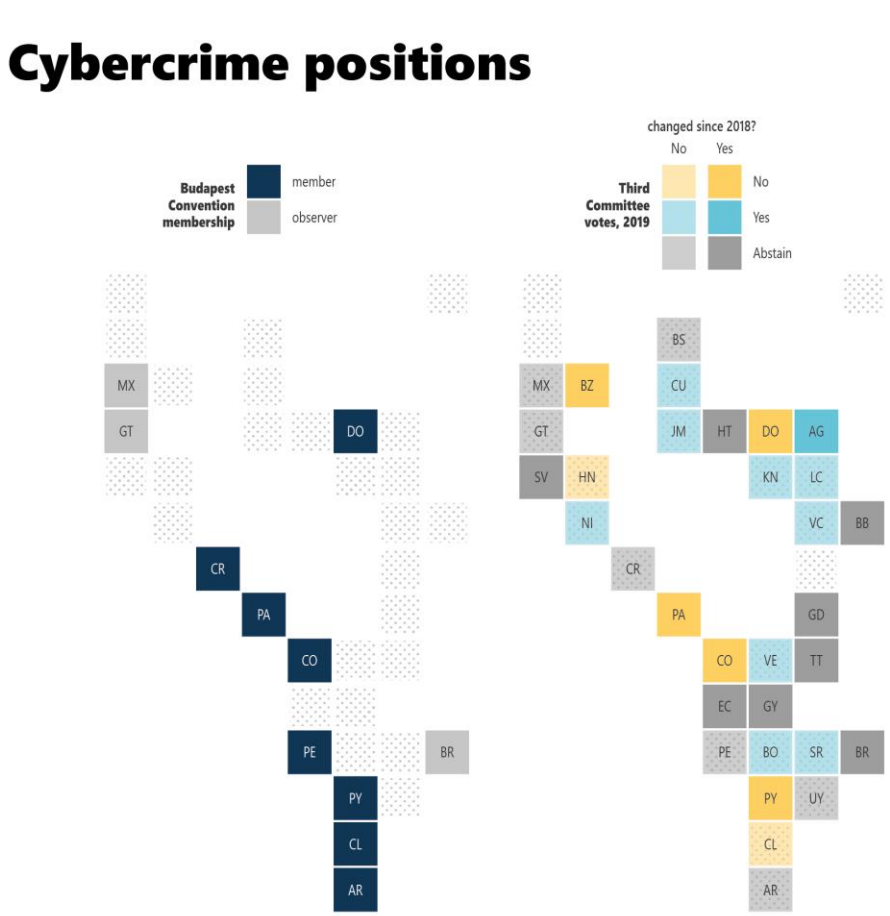
[110] United Nations Third Committee (2018) 'Countering the use of information and communications technologies for criminal purposes' draft resolution A/C.3/73/L.9 https://undocs.org/en/A/C.3/73/L.9

[111] United Nations Commission on Crime Prevention and Criminal Justice (2015) 'Non-Paper submitted by Brazil reflecting its views on the issue of cybercrime' E/CN.15/2015/CRP.5 https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_24/ECN152015_CRP5_e_V1503408.pdf

[112] United Nations Third Committee (2018) 'Countering the use of information and communications technologies for criminal purposes' draft resolution A/C.3/73/L.9 https://undocs.org/en/A/C.3/73/L.9

[113] https://www.apc.org/sites/default/files/Open_letter_re_UNGA_cybercrime_resolution_0.pdf

[114] United Nations Third Committee (2019) draft resolution 'Countering the use of information and communications technologies for criminal purposes' draft resolution' A/C.3/74/L.11/Rev.1 https://undocs.org/en/A/C.3/74/L.11/Rev.1



4.3. Free and open rule-based internet

Convergence on principles to govern a free and open rule-based Internet is also visible from initiatives outside of the United Nations, such as the Paris Call for Trust and Security in Cyberspace. Many Latin countries joined French President Macron's Paris Call in 2018.

The Paris Call was endorsed and supported by Mexico, Chile, Colombia, Argentina, Peru, and Panama, with Brazil being a notable absentee.[115] The Paris Call reiterates the principles established over almost a decade of work by multilateral and multi-stakeholder fora. Some observers have put it forward as a "third way" to govern the Internet.[116] While the Paris Call is not legally binding, participation in the call is a promising indicator of convergence with European values on governing a free and open Internet that is rule-based. Caution, however, is warranted; Latin American declarations of liberal values in multilateral fora haven't always translate into domestic policy.[117] As previously mentioned, civil societies remain sceptical of policies that claim to protect online freedom of expression and privacy but remain

[115] France Ministry for Europe and Foreign Affairs (2018) 'Paris Call of 12 November 2018 for Trust and Security in Cyberspace' 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

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

[117] Kurtenbach, Sabine (2019) 'Latin America – Multilateralism without Multilateral Values' Giga Focus, 2019-7

dead letter on paper. Without sufficient accountability mechanisms, granting states more legitimacy to govern the Internet could potentially be dangerous in Latin America.

5. Navigating between the US and China

Latin America has a complicated relationship with the two dominant cyber forces in the world, the US and China. From an intertwined history with the United States, to an increasing interest and dependency on China, both engagements are examined here in order to explore how the region positions itself between these countries. This also helps set a picture for the emerging "third way" approach that was mentioned above under the Paris Call initiative. It helps to develop an understanding of how Europe can engage with Latin America and its shared partnerships.

5.1. United States

Latin America's historic and structural ties with the United States are a common thread throughout this paper. Latin America has historically been very dependent on the US, and this has been no less true for digital issues. First, the whole region has been physically linked to the US' digital infrastructure from the onset. All of Latin America's international traffic is routed through the US and many of the content generated in the region is hosted in the United States. The problematic state of this single point of dependency became apparent when the Snowden leaks revealed the scale and ease of surveillance on the region. Second, the US has a front row seat when it comes to observing how the region organises itself through the OAS. The US provides a large amount of funding to the OAS, which has been the driving force for regional integration that includes the northern hemisphere. Third, the US has been instrumental in cyber capacity building in the region. It was the driving force behind the first cybersecurity strategy in 2004 and the first cyber CBM. In bilateral engagements, the US is strongly engaged in the region in cyberdefence.

However, the US' role in the region is evolving. First, countries on the continent are reducing their dependency on US infrastructure. The construction of a submarine cable connecting Latin America with Europe, the EllaLink cable, is expected to significantly decrease traffic dependency on the United States.[118] Second, while the US' policy on Latin America could always be characterised as one of "benign neglect", under President Trump, the US' participation in the region has decreased to the level of disregard.[119] Important ambassadorial positions in Latin America were not filled for a long time and the Trump administration hardly makes any visits to the region. For the first time ever, there was no president of the United States present at the 8th OAS Summit of the Americas in Lima in 2018. Ironically, and also for the first time ever, there was a Chinese observer present at that summit.[120] This neglect speaks to the third point on the US' lead on cybersecurity for the region. Canada seems to have taken over this role in some respects. Canada has become the second-largest funding nation to the OAS after becoming a member in 1990. It is the biggest donor to the OAS' cybersecurity programme and was the

[118] European Commission (2018) 'BELLA: A new digital data highway between Europe and Latin America' Digital Single Market https://ec.europa.eu/digital-single-market/en/news/bella-new-digital-data-highway-between-europe-and-Latin America
[119] Nolte, Detlef (2018) "Trump and Latin America : Between Monroe doctrine and Disregard" GIGA Focus, 2019-3
[120] Nolte, Detlef (2018) "Trump and Latin America : Between Monroe doctrine and Disregard" GIGA Focus, 2019-3

main financial contributor to the establishment of CSIRTAmericas. Meanwhile, the US contributed 16 percent less funding to the OAS in 2018.[121]

While reducing dependencies, the US is also losing strategic interest. When the US withdrew from the Trans-Pacific Partnership (TPP) in 2018, it gave up a strategic advantage in the region against China.[122] When the partnership was resurrected as the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) without the US in 2018, it created one of the largest free trade zones with 11 countries across the Pacific.[123] While many of the US' economic interests are safeguarded through bilateral free trade agreements with various Latin American countries,[124] it is allowing the region to diversify its trade and explore new partnerships, among others with China.

5.2. China

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.[125] Both the MERCOSUR and Pacific Alliance trading blocs have generally welcomed China's trade and investment in Latin America. China is the largest trade partner for Chile, Argentina, and Peru, and Chile and Peru are part of the Chinese Free Trade Agreements network.[126] Many see the benefits of a regional alliance to interact with China, and some even see the potential of a MERCOSUR-Pacific Alliance bloc as it provides countries with a greater advantage in negotiations.[127] While Chinese expertise and loans can jumpstart e-commerce, there is unease over the increasing presence of Chinese infrastructure in the region. Some of the more developed countries are receiving cheap electronic equipment and have accepted Chinese support for increased digitalisation.[128] 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 C.E.I.E.C. and Huawei.[129] Replicas are also being sold to Bolivia and Venezuela, and Argentina also seems eager to buy into Chinese surveillance technology.[130]

Bonds with Latin America are not just strengthened through trade but also politically. Political cooperation between China and Latin America runs through CELAC, which hosted several China-CELAC

[121] Meyer, Peter J. (2018) 'Organization of American States: Background and Issues for Congress' Congressional Research Service https://fas.org/sgp/crs/row/R42639.pdf
[122] Nolte, Detlef (2018) "Trump and Latin America : Between Monroe doctrine and Disregard" GIGA Focus, 2019-3
[123] Partner countries are Australia, Brunei, Japan, Malaysia, New Zealand, Singapore, Vietnam, Peru, Mexico, Chile and Canada
[124] 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)
[125] Gonzalez, Anabel (2018) 'Latin America-China Trade and Investment Amid Global Tensions' The Atlantic Council's Adrienne Arsht Latin America Center https://www.atlanticcouncil.org/wp-content/uploads/2018/12/Latin America-China-Trade-and-Investment-Amid-Global-Tensions.pdf
[126] Guerra-Baron, Angelica (2018) 'China and South-America : the Pacific Alliance' Impakter https://impakter.com/china-and-south-america-the-pacific-alliance/
[127] Marczak, Jason (2018) 'Latin America's Future Begins with the Pacific Alliance' Atlantic Council
[128] Lynch, Justin (2018) 'When South American Nations look for Cyber Help, China Looms' Fifth Domain https://www.fifthdomain.com/dod/cybercom/2018/11/29/when-south-american-nations-looks-for-cyber-help-china-looms
[129] Mozur, Paul; Kessel, Jonah M.; Chan, Melissa (2019) 'Made in China, Exported to the World: The Surveillance State' The New York Times https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html
[130] Garisson, Cassandra (2019) ''Safe like China': In Argentina, ZTE finds eager buyer for surveillance tech' Reuters https://www.reuters.com/article/us-argentina-china-zte-insight/safe-like-china-in-argentina-zte-finds-eager-buyer-for-surveillance-tech-idUSKCN1U00ZG

summits. At the 2015 Summit, CELAC made a 2015-2019 cooperation plan with China. In this plan, CELAC members pledged to "enhance dialogue and collaboration on Internet governance and cyber security" and work together to "build an Internet space that features peace, security, openness and cooperation".[131] 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 Panama and the Dominican Republic have accepted.[132] Former Chilean President Bachelet also proposed the building of a trans-Pacific fibre optic Internet cable between China and Chile at the 2018 summit.[133] It would link the Asian and South American continents for the first time, similar to the ongoing construction of the EU-Brazilian cable. Japan is also an interested party for the trans-Pacific connection. Chile will decide in late 2020, after it has launched the bid to build the cable, whether it will enter through China or Japan.[134] Mexico has promised to continue regional engagement with China under its CELAC chairmanship and will hold a CELAC-China Ministerial Forum at the end of 2020.[135]

There is risk of value distortion that comes with such cooperation and trade that is a matter of concern for human rights in the region. Ayuso, Gratius and Serbin do not see this growing bond with China as having caused an assimilation of Chinese values yet, as identification with Western liberal values seems to prevail in the government and active citizenship.[136] Civil society in Latin America, however, is worried, especially in light of the recent COVID-19 pandemic. China has built possible digital solutions to combat the pandemic that are far from being respectful of human rights. Digital rights organisations warn of the possible application of these tools by Latin American states.[137]

6. The EU and Latin America

Latin America has always been a key ideological ally for the EU to address global challenges.[138] Both regions have been perceived as having more soft power than hard and as being committed to liberal values and to the strengthening of the rule-based order through multilateral institutions.[139] The strong strategic partnership between the EU and Latin America has provided a great foundation for building cooperation in cyber diplomacy. This does not have to start from scratch, as it will become apparent that the EU and Latin America have already cooperated on cybersecurity issues in numerous ways.

[131] China-CELAC Forum (2015) 'Cooperation Plan 2015-2019' http://www.chinacelacforum.org/eng/zywj_3/t1230944.htm
[132] Nolte, Detlef (2018) "Trump and Latin America : Between Monroe doctrine and Disregard" GIGA Focus, 2019-3
[133] Nolte, Detlef (2018) "Trump and Latin America : Between Monroe doctrine and Disregard" GIGA Focus, 2019-3
[134] Van der Spek, Boris (2019) 'Chile to Build First Fiber-Optic Submarine Cable Between South America and Asia' Chile Today https://chiletoday.cl/site/chile-to-build-first-fiber-optic-submarine-cable-between-south-america-and-asia/
[135] González, Oscar Brandon Pérez (2020) 'Mexico in CELAC: the revitalization of Latin America and the Caribbean' Latin American Post https://latinamericanpost.com/31708-mexico-in-celac-the-revitalization-of-Latin America-and-the-caribbean
[136] Serbin, Andrès & Serbin Pont, Andrei (2019)'Why should the European Union have any relevance for Latin America and the Caribbean?' EU-LAC foundation
[137] 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/
[138] Ruano, Lorena (2018) 'Dealing with Diversity: the EU and Latin America Today' Chaillot Paper, EUISS
[139] Serbin, Andrès & Serbin Pont, Andrei (2019)'Why should the European Union have any relevance for Latin America and the Caribbean?' EU-LAC foundation

6.1. Strategic partnership with the EU

The EU and Latin America have a long history and have managed to transform their relationship into a strategic partnership. The establishment of this strategic partnership was formalised at the first bi-regional summit in 1999, where a shared community of values and interest was at the centre of the partnership. This became a recurring mantra after the Cold War.[140] With the EU being the third-largest trading partner for the region, EU-Latin American cooperation has mostly concentrated on trade and North-South cooperation. However, there is much potential for cooperation in other areas of interest, which the EU highlighted in its 2019 joint communication. In the communication, the EU proposes strengthening its political partnership with Latin America. Advancing the digital economy is prominently mentioned, and cybersecurity is mentioned as a promising area for cooperation. Cooperation on the global governance of cybersecurity and hybrid threats is also explicitly mentioned.[141] All in all, the communication lays the foundations for enhanced cooperation in cyberspace issues. This is also accompanied by funding, which the 2019 Council Conclusions mentioned to be included in the next Multiannual Financial Framework.[142] The partnership communication also coincided with the finalisation of the EU-MERCOSUR Free Trade Agreement in 2019.[143] This trade agreement was at a stalemate for 20 years. The Mercosur trade agreement is important for the strategic partnership, and the sudden completion can be seen as another sign of Latin America's appetite for diversification. There is no mention of data flows and data security regulation in the agreement, as it was not yet relevant when the negotiations were first initiated, but the 2019 strategy highlighted the need for regulatory alignment to advance digital cooperation.

Cybersecurity cooperation on a bi-regional level has been difficult. While the OAS is the most active regional organisation on cybersecurity, the EU has not established a dialogue with the organisation that also includes the US and Canada. In recent informal high-level dialogues with the OAS, however, cybersecurity was mentioned as a potential new area for cooperation.[144] The EU is, after all, a permanent observer to the OAS and officially it has had a framework for inter-institutional dialogue with the OAS since 2009.[145] The EU has, though, favoured political coordination with the region through CELAC, which it designated as its official regional interlocutor when it was created in 2011. In 2015, the EU High Representative Frederica Mogherini attended CELAC's 2015 Costa Rica Summit, where she stressed the need to strengthen the EU-CELAC relationship.[146] A few months later, the 2015 bi-regional EU-CELAC summit was organised in Brussels. At this EU-CELAC summit, an action plan emerged that also included

[140] Kurtenbach, Sabine (2019) 'Latin America – Multilateralism without Multilateral Values' Giga Focus, 2019-7

[141] European Commission (2019) 'European Union, Latin America and the Caribbean: joining forces for a common future' Joint Communication to the European Parliament and the Council https://eeas.europa.eu/sites/eeas/files/joint_communication_to_the_european_parliament_and_the_council_-_european_union_latin_america_and_the_caribbean_-_joining_forces_for_a_common_future.pdf

[142] European Council (2019) 'Council Conclusions on the Joint HR/Commission Communication on EU relations with Latin America and the Caribbean, "Joining forces for a common future' 9241/19 https://www.consilium.europa.eu/media/39346/eu-lac.pdf

[143] European Commission (2019) 'New EU-MERCOSUR Trade agreement in principle' http://ec.europa.eu/trade/policy/in-focus/eu-mercosur-association-agreement/

[144] Shared by European External Action Service officials in interviews with the author

[145] Priorities according to this framework were the promotion and protection of Human rights, integral development, strengthening of democracy and other transnational issues. 'Memorandum of Understanding between the European Commission and the General Secretariat of the Organisation of American States' http://www.der.oas.org/Permanent_Observers/MoU%20EU.pdf

[146] Stevens, Christine (2015) 'Region to Region Cooperation: EU and CELAC' Egmont Institute

a digital component.[147] The EU-CELAC summit planned for October 2017 had to be postponed at the request of Latin America due to the conflict over Venezuela, and only took place in 2018 between foreign ministries. The Mexican CELAC presidency has, however, expressed its intention to organise another EU-CELAC summit and strengthen the partnership with the EU.[148]

Despite good intentions, the Latin American regional heterogeneity makes a symmetrical relationship very difficult.[149] This is not necessarily problematic. Research by the EU-LAC Foundation shows that over the years, a multi-level institutional structure has been created between the two regions. An enormous amount of dialogues and fora are spread over several themes and levels (inter-regional, sub-regional, bilateral, and local).[150] Many state and non-state actors seem to be contributing to building a horizontal agenda. Unfortunately, the fragmentation of these efforts makes partnership less visible. The amount of effort and political capital that is invested in these dialogues contrasts with the limited visibility of EU actions in Latin America. The many dialogues also seem to have less of an impact at the global level as both regions seem to rarely coordinate their positions.[151]

6.2. Cyber cooperation

As the 2019 Joint Communication stressed, cybersecurity can be a promising area for cooperation. This cooperation is not in its infancy - there is already cooperation on cybersecurity and other digital policy issues - but it is spread over several themes, pillars, and layers, led by several institutions in the European system. The following is an overview of current EU efforts in cybersecurity policy development and capacity building on bi-regional and bilateral levels.

The EU has contributed to several policy development efforts in the region. Through the European participation in the eLAC ministerial conferences of the United Nations Economic Commission for Latin America and the Caribbean (CEPAL), the European Commission was actively involved in setting the region's 2020 digital agenda. This also contains cybersecurity objectives in the region's action plan.[152] In the past, the European Commission successfully managed to set "ICT for Development" on this eLAC agenda.

[147] European Council (2015) 'EU-CELAC Action Plan' https://www.consilium.europa.eu/media/23757/eu-celac-action-plan.pdf

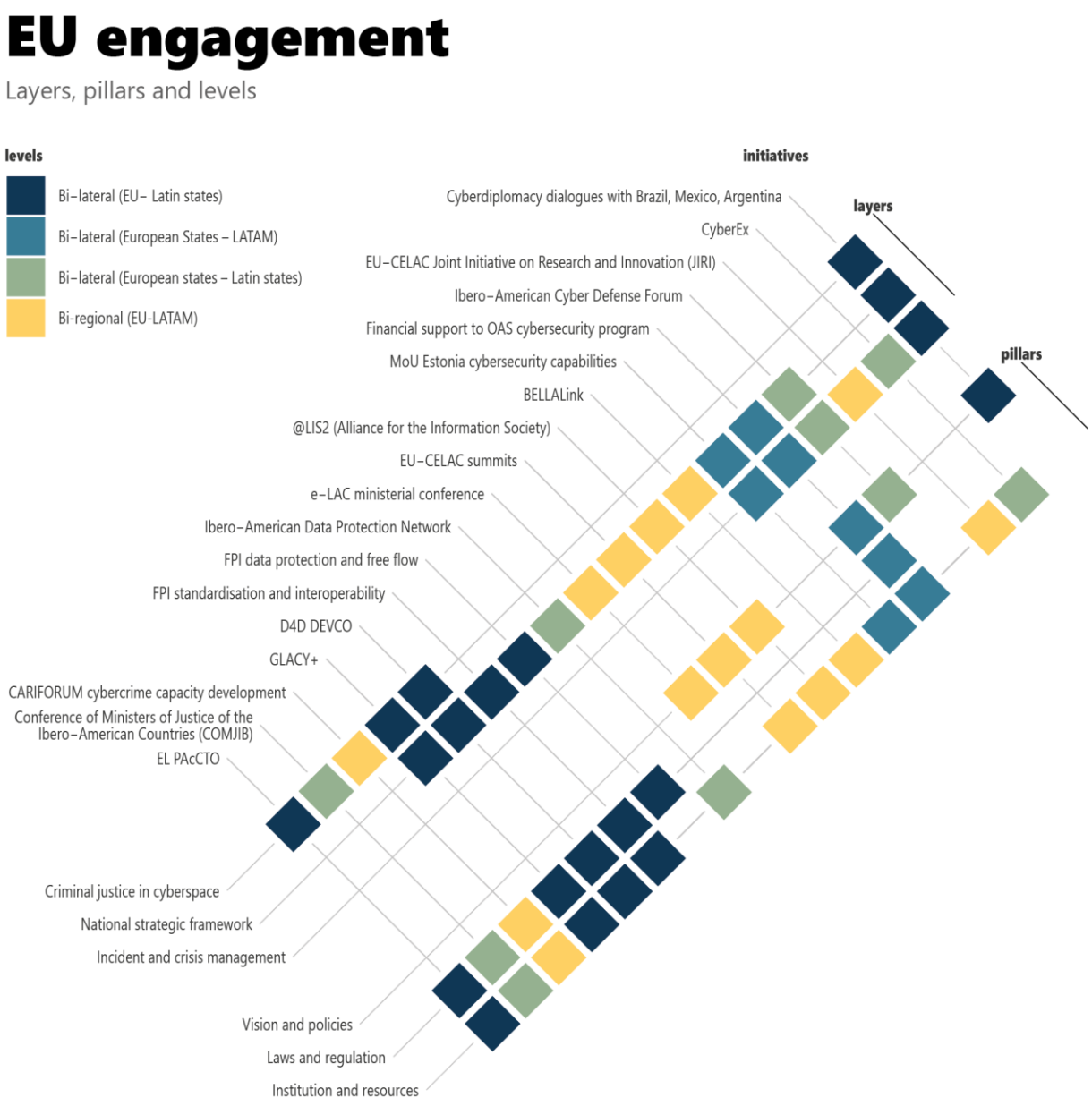
[148] Gobierno de México (2020) 'Foreign Secretary Ebrard Presents Mexico's Work Plan as CELAC President Pro Tempore' Press release https://www.gob.mx/sre/prensa/foreign-secretary-ebrard-presents-mexico-s-work-plan-as-celac-president-pro-tempore?idiom=en

[149] Serbin, Andrès & Serbin Pont, Andrei (2019)'Why should the European Union have any relevance for Latin America and the Caribbean?' EU-LAC foundation

[150] To see all involved stakeholders in EU-LAC cooperation, the EU-LAC Foundation created a mapping tool https://eulacfoundation.org/en/search/mapeo
Serbin, Andrès & Serbin Pont, Andrei (2019)'Why should the European Union have any relevance for Latin America and the Caribbean?' EU-LAC foundation

[151] Serbin, Andrès & Serbin Pont, Andrei (2019)'Why should the European Union have any relevance for Latin America and the Caribbean?' EU-LAC foundation

[152] CEPAL (2018) 'Follow-Up Mechanism for the Digital Agenda for Latin America and the Caribbean (eLAC2020) for the Period 2018-2020' LC/CMSI.6/3/Rev.2
https://repositorio.cepal.org/bitstream/handle/11362/43329/S1800464_en.pdf?sequence=4&isAllowed=y



The European @LIS2 programme, the Alliance for the Information Society, run by the EU's DG on development cooperation until 2013, was actively involved in implementing this objective.[153] Influence on the digital economy was also a priority in the 2015 EU-CELAC action plan, which focused on cooperation between both regions to reduce the digital divide. One of the goals was to increase the compatibility of regulatory frameworks for digital communication, another was to support the region in rolling out broadband.[154] As has been noted, EU cooperation in Latin America is more effective on a

[153] European Commission (2013) 'International Cooperation and Development in Latin America - @LIS II - ALliance for the Information Society' https://web.archive.org/web/20190629161811/https://ec.europa.eu/europeaid/regions/Latin America/lis-ii-alliance-information-society_en

[154] European Council (2015) 'EU-CELAC action plan' https://www.consilium.europa.eu/media/23757/eu-celac-action-plan.pdf

bilateral level. Since 2018, the European Commission Directorate General for Communications Networks, Content and Technology (CONNECT) has led several projects in Latin America funded through the Partnership Instrument project for International Digital Cooperation.[155] One cluster of this project focuses on personal data protection, for which it is cooperating with Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico, and Uruguay.[156] Another focuses on standardisation and interoperability of ICT services across international borders, for which it is cooperating with Brazil.[157] The EU Cyber Diplomacy and Resilience Clusters, implemented by the EU Cyber Direct, is also funded through the Partnership Instrument project.[158] The EU has engaged in several cyber dialogues with Brazil[159] and there have been digital dialogues with Mexico and Argentina.[160]

The EU has engaged in building policies, regulations, and capacities on cybercrime in Latin America through two specific projects. The first is the Global Action on Cybercrime (GLACY and GLACY+) project, which started in Latin America in 2013. This has the goal of improving cybersecurity policy and cybercrime legislation. This project, funded by the EU and implemented by the Council of Europe, also assists Latin countries to adopt the Budapest Convention.[161] The second is the Europe Latin American Assistance Programme against Transnational Organized Crime (EL PAcCTO). This project focuses on building capacities against cybercrime by improving police cooperation with the justice system. EL PAcCTO is a joint initiative of EU and Latin American countries financed by the EU.[162]

The EU also included cybercrime capacity development for CARIFORUM member states in the 11th European Development Fund. This will strengthen capacities in the Caribbean countries to battle cybercrime once it starts in 2020. This project will be implemented by CARICOM/IMPACS, which received a direct funding award.[163]

The European Commission Directorate General on Development Cooperation (DG DEVCO) has been focusing on building digital capacities. Its recent Digital for Development (D4D) guidelines, created in 2017, have the objective to mainstream digital technologies and services into the EU's development

[155] European Commission Service for Foreign Policy Instruments 'Partnership Instrument Project: International Digital Cooperation' last accessed 19/02/2020 https://web.archive.org/web/20200219012059/https://pimap.eu/admin/project/82/pdf

[156] European Commission 'Digital Single Market policy for the Americas' Directorate General for Communications Networks, Content and Technology (DG CONNECT) last accessed 12/02/2020 https://ec.europa.eu/digital-single-market/en/americas

[157] European Commission 'Digital Single Market policy for the Americas' Directorate General for Communications Networks, Content and Technology (DG CONNECT) last accessed 12/02/2020 https://ec.europa.eu/digital-single-market/en/americas

[158] https://eucyberdirect.eu/

[159] As bilateral cooperation has been very active with Brazil, a separate EU Cyber Direct paper dives deeper into the EU's engagement on cyber security and diplomacy with Brazil. Ebert, Hannes & Groenendaal, Laura (2020) 'Brazil's Cyber Resilience and Diplomacy; The Place for Europe' Digital Dialogue series https://eucyberdirect.eu/content_research/brazils-cyber-resilience-and-diplomacy-the-place-for-europe/

[160] European Commission (2018) 'Promoting the Digital Single Market in the Latin America & the Caribbean region' Directorate General for Communications Networks, Content and Technology (DG CONNECT) presented at the Workshop on Digital Cooperation between the European Union and Latin America & the Caribbean

[161] Council of Europe 'Global Action on Cybercrime' last access 16 February 2020 https://www.coe.int/en/web/cybercrime/glacy

[162] 'What is EL PAcCTO?' http://www.elpaccto.eu/en/

[163] European Commission (2017) 'Action Document for Capacity Development for CARIFORUM Member States on Financial Compliance, Asset Recovery and Cybercrime' https://web.archive.org/web/20190531015337/https://ec.europa.eu/europeaid/sites/devco/files/aap-financing-regionalcaribbean-annex2-2017-20171211_en.pdf

policy.[164] Mainstreaming these efforts into existing initiatives is ongoing. Under D4D there are no immediate Latin-specific initiatives for cybersecurity capacity development. Since the OAS has already taken a holistic approach to build resilience in Latin America, a focusing effort is needed not to duplicate any efforts or create competing development programmes.

The cooperation between the two regions also has a strong link via European and Latin research and education networks, for which the EU's DG Research and Innovation is responsible. A framework for innovation cooperation as well as a Common Research Area is being developed by the EU-CELAC Joint Initiative on Research and Innovation (JIRI). Concrete joint research activities have been implemented between 2013 and 2017 under the ERANet-LAC project, which transformed into the EU-CELAC interest group that coordinates applications for Horizon 2020 funding. This is supported by the Spanish Foundation for Science and Technology.[165] These research connections are being physically strengthened through the development of the previously mentioned BELLA (Building Europe Link to Latin America). Coordinated by RedCLARA (Latin American Cooperation of Advanced Networks) and GEANT (the European Research and Education network) and funded by the European Commission, the BELLA is an underwater fibre optic cable that will connect Latin America and Europe. With this cable, the links between research and education networks in the two continents will be strengthened, to boost scientific, cultural and business exchanges. The cable will also be extended throughout Latin America, to improve the interconnectivity between Latin American networks. The cable is expected to be operational in 2020.[166] It is also worth mentioning that the European Commission supported the development of this RedCLARA research network, which aims to connect Latin America's academic computer networks. @LIS, the predecessor of the previously mentioned @LIS2 project that worked on ICT for development, supported the creation of the RedCLARA network in 2004.[167]

The role of EU member states in Latin America is also noteworthy. Of the EU member states, Portugal and Spain have been historically most active in bilateral cooperation with the region. Most notably, these member states have contributed through the Conference of Ministers of Justice of the Ibero-American Countries (COMJIB), which facilitated the signing of the Ibero-American cooperation agreement in 2014 on research, assurance, and securing of evidence in cybercrime.[168] They also assisted Latin American states in adopting data protection standards similar to the European Union's General Data Protection Regulation ("GDPR") through the Ibero-American Data Protection Network. The Latin countries that are members of this network, Argentina, Chile, Colombia, Mexico, Peru, and Uruguay, adopted new data protection standards in the past few years based on the Ibero-American Standards on Data Protection.[169] Spain also contributes to improved incident response capacities through its

[164] European Commission Staff Working Document (2017) 'Digital4Development: mainstreaming digital technologies and services into EU Development Policy' https://ec.europa.eu/international-partnerships/system/files/swd-digital4development-part1-v3_en.pdf

[165] ERANet-LAC Strategic roadmap for Joint Activities https://www.eucelac-platform.eu/sites/default/files/documents/eranet-lac_strategic_roadmap_for.pdf

[166] European Commission (2018) 'BELLA: A new digital data highway between Europe and Latin America' Digital Single Market https://ec.europa.eu/digital-single-market/en/news/bella-new-digital-data-highway-between-europe-and-Latin America

[167] European Commission (2013) 'International Cooperation and Development in Latin America - @LIS II - ALliance for the Information Society' https://web.archive.org/web/20190629161811/https://ec.europa.eu/europeaid/regions/Latin America/lis-ii-alliance-information-society_en

[168] Justice Ministers of Ibero-American Countries (2014) 'Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en material de Ciberdelincuencia' Office of Secretary-General

[169] Ibero-American Data Protection Network (2017) 'Standards for Data Protection for the Ibero-American States'

annual international cyber incident exercise, CyberEx, which it organises with the OAS.[170] The OAS' cybersecurity programme, run by CICTE, has also received financial support from the governments of Spain, Estonia, and the United Kingdom.[171] Estonia even signed a Memorandum of Understanding with the OAS to promote the development of cybersecurity capabilities in the Americas.[172]

The existing cooperation of European institutions and EU member states with Latin America on cybersecurity is apparent from the myriad projects that build capacities and influence cyber policy based on a shared set of values. They are a great jumping off point to expand a comprehensive bi-regional strategy for fostering global stability in cyberspace.

Conclusions

This digital dialogue has painted a picture of the complex interactions in Latin America and the priorities for the region that will facilitate the building of a secure and rights-based global cyberspace. Despite a certain heterogeneity in the region, there are effective regional cooperation mechanisms that strengthen the region against digital threats. The OAS successfully coordinates the development of states' cyber resilience. It has worked on building trust and battling cybercrime, while focusing on certain safeguards for human rights. Trade organisations like the MERCOSUR and Pacific Alliance are adapting the region's economy to the digital reality and bringing a mindset where cyber resilience is necessary to protect the economy. Internationally, Latin countries have managed to agree on some common Latin positions on cyberspace issues through CELAC and former UNASUR collaborations.

The region is marked by changing alliances and clashing ideologies, making it hard to sustain these political cooperation mechanisms. Recently, the humanitarian crisis in Venezuela caused a rift in the region, with the implosion of UNASUR as a consequence. CELAC's future was uncertain for a few years, partly due to the same discrepancies. The 2020 commitment of the Mexican CELAC leadership to strengthen the unity of CELAC countries has the power to create a united Latin voice in multilateral fora, elevating it beyond the regional polarisation of left-wing and right-wing governments. It remains to be seen whether this centrist "third way" approach under the Mexican presidency will work.

What these frictions mean for a united Latin voice on the international governance of cyberspace is unclear. States like Venezuela, Cuba, Nicaragua, and Bolivia seem to be going against the positions of most Latin states in UN discussions, pledging their support for a new cybercrime resolution and uttering the need for a new treaty on state behaviour in cyberspace. An analysis of UN statements at the recent OEWG, however, confirms that all countries in the region have expressed views similar to the European Union, namely that the Internet needs to remain free and open, that the norms agreed under the 2015 UNGGE need to be implemented, and that a secure cyberspace needs to be rules- and rights-based. Many Latin states expressed the need for a clear dialogue on the application of international law in cyberspace and some like Mexico proposed a role for the UN to create an implementation mechanism for norms. They also expressed discomfort with the growing weaponisation of cyberspace. Even Brazil, which has recently seen a rapprochement to US President Trump under President Bolsonaro, made critical remarks that the applicability of international law does not legitimise cyberconflict. This

[170] INCIBE-CERT 'International CyberEx' last accessed 18/02/2020 https://www.incibe-cert.es/en/international-cyberex

[171] Organization of American States (OAS) (2017) Annual Report of the CICTE to the 48th session of the General Assembly (approved at first plenary session held on May 3rd, 2018)

[172] Organization of American States (OAS) (2015) ' Estonia Contributes 100,000 dollars to OAS Cyber Security Program' http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-107/15

perspective contrast with the US' "persistent engagement" strategy, with which the US seeks to operate militarily in cyberspace within the confines of international law.

Latin states seem to be exploring new partnerships beyond their strained marriage with the US. This is in spite of their great cooperation with the US within the OAS that has yielded much in terms of cyber resilience and trust building. There has been a noticeable cordiality towards China in the last decade. Fears of value distortion through Chinese influence might be unfounded, as there seems to be a commitment from Latin countries to liberal values, particularly in discussions on Internet governance, but civil societies remain sceptical of declarations that claim to protect online freedom of expression and privacy. The decline in Internet freedom in the region does not bode well. There is, however, great potential for Latin American Internet governance that respects online freedoms, if the states allow cooperation with non-governmental stakeholders to create rights- and rules-based stability in cyberspace.

This paper showed that the EU has a number of engagements with Latin America on cybersecurity. The OAS is the main driver in the region for cybersecurity, but the EU has not established a dialogue with the organisation, as it leaves little wiggle room for participating in its cybersecurity programme without exchanging European values. It is exploring possibilities for cooperating with the OAS on cybersecurity but has so far preferred cooperation with CELAC since 2011. Regardless of the lacking regional cooperation, there has always been a multidimensional relationship with Latin America. The existing cybersecurity initiatives that the EU has launched in Latin America have strengthened democratic institutions and rule of law. They have supported the developments of national regulations and policies to counter threats in cyberspace and aimed to create a healthy digital society with all stakeholders. These efforts have the potential to fit a wider agenda for the EU's partnership with Latin American. The EU's partnership with Latin America has always shared liberal values, which are not merely motivated by economic interests or neighbourhood security. There is ample opportunity to build a secure and rights-based global cyberspace in partnership with Latin America. The willingness to coordinate positions at the international level and the maturity to cooperate on building cybersecurity capacities with the like-minded region is there.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

DIGITAL DIALOGUES

are a series of research papers providing an overview of selected issues, policies and institutions of the EU's main strategic partners.

EU CYBER DIRECT

This project is funded by the European Union.