Digital Security in Latin America Research Group

Beyond the Usual Suspects: Latin American Cyber Security

Workshop Report

March 2023

KEY POINTS

- There are many restrictions to researching cyber security in Latin America. Though more courses are becoming available, challenges remain as research areas remain siloed and there is little interdisciplinarity.

- Cyber security policy in the region is for the most part reactive. It draws from international best practices but is not always adjusted to fit the Latin American context.

- The report highlighted a duality between Latin American approaches to cyber security and relationships with the west in shaping them. Partnerships with western states, and in turn the emulation of western state practice, are often seen as measures of cyber security maturity or capability. However, there also exists an appetite amongst Latin American states to pursue their own independent cyber security approaches.

- Processes of political change and the impacts that these have on issues of cyber security, must be understood against a broader backdrop of historical and current conflict.

- When it comes to the practice of cyber security, a divide exists between the policy and grassroots level. Strategies and policies may satisfy international standards and requirements, but may do little to address local realities and concerns. The cyber security of the ‘everyday’ in Latin America needs further inquiry.

TABLE OF CONTENTS

CONTEXT

On the 1st of December 2022, the Digital Security in Latin America Research Group (DSLA) held an online workshop with 25 participants primarily from academia and civil society. The main aim was to start connecting and building a community of people interested in the topics of cyber and digital security in the context of Latin America, facilitating interdisciplinary learning and bridging different research communities. Literature on cyber security in Latin America is relatively limited compared to the abundance of knowledge that exists in other regions, though it is nevertheless emerging. Building on this growing area, we wanted to carry out a workshop that brought together scholars and practitioners working on these subjects.

The event was therefore an opportunity to get individuals from diverse backgrounds who have been researching and operating in this space to participate in discussions around two main topics: the current state of cyber security research in the region, and the impacts of political change in this area. Through these conversations we were able to get an initial sense of some of the challenges and particularities of cyber security in the Latin American context. It has also prompted many ideas for further research.

Before delving into some of these points, it is worth noting some caveats. First, though we use the term "Latin America", we acknowledge that there is no "Latin American approach" per se. There may be similarities, but ultimately there are clear differences between countries and the diverse cultures and populations. We are therefore careful to not generalise opinions expressed throughout the discussions. Second, though we tried to bring in diverse perspectives, we cannot say that the discussions reflect universal views. Instead, they should be seen as reflections of the experiences of those who took part in the workshop. Third, the summary that follows is a reflection of the points discussed throughout the workshop and not necessarily our own opinions on the subject.

Finally, we recognise that the use of ‘cyber security’ vs ‘digital security’ is an important distinction in many academic fields. We built a workshop using the terminology of ‘cyber security’ as an initial starting point, but used the terms interchangeably in the discussions and subsequently this report. We are trying to build bridges between different research communities, and therefore wanted participants to use the language they preferred. We look forward to conducting future research to distinguish the similarities and differences of such terminology.

The workshop was divided into two sessions. At the start of each session, we invited a speaker to voice their perspectives on the topic as a way to spark conversations in the subsequent break out rooms. The topic areas covered in the sessions and the sub questions moderators used for guidance included:

What is the current state of research on cyber security in Latin America?	**Political change and how that impacts cyber security.**
• From your experiences in your given field, how would you describe the current research agenda for cyber security? • Is there coordination in cyber security policy across Latin America? • Is cyber security approached in relation to physical security, particularly in countries which have come through conflict or political upheaval? • Is there a gap in technical knowledge in specific countries? What can universities do to support future professionals and academics?	• Is cyber security on the agenda of incoming political leaders in Latin America? • Is there increasing pressure from civil society to improve cyber security? • Is there pressure to comply with international standards in relation to cyber security and data protection?

This report provides a summary of the responses to the questions above and the discussions that emerged following the speaker keynotes. Our hope is that this can provide a starting point for further conversations and inquiry into the topic.

1) CHALLENGES IN CYBER SECURITY RESEARCH AND PRACTICE IN LATIN AMERICA

The challenges associated with the research and practice of cyber security in Latin America were a recurring theme throughout the first session of the workshop. Although each country will have different types of challenges, some of the issues mentioned throughout the discussions could be seen across different countries in the region. The following section will look first at the challenges around research on cyber security in Latin America, and then at the challenges around cyber security policy making. Most of this section is based on the responses given to the first topic: *What is the current state of research in cyber security in Latin America*?

Challenges in Research

One of the major challenges highlighted throughout the discussions were the limited opportunities for cyber security research in the region. This ranges from limited funding availability to a lack of available courses on these topics, and limited links between northern and southern hemisphere universities (links that could facilitate and support this type of research). For instance, one participant commented on how scarce cryptographic courses seem to be in the region, whilst another noted that those who were interested in these topics were often forced to find these courses abroad (outside of Latin America). Furthermore, some participants noted that avenues for collaboration are limited and highlighted the challenges of information sharing when there are few channels for academic cooperation, and even less for government and academic partnerships. This lack of opportunity arguably makes it harder for these countries to overcome the cyber security skills gap.

Some countries like Chile[1] and Uruguay[2], have started to provide more learning opportunities. However, there are still many hurdles to overcome. For instance, discussions in the workshop highlighted the lack of interdisciplinary training around cyber security in Latin America. Although technical courses are of the utmost importance, the participants recognised that cyber security is more than just the technical, and that it requires careful consideration of human factors, an element that still needs to be worked upon. As one participant noted, it is "hard to bridge the gap between hard sciences and political sciences in approaching cyber security but multi-disciplinary approaches could help". Few courses can overcome the divide between the different lenses around cyber security. Indeed, when we reached out to some scholars outside of the 'technical' or 'policy' realm to join the workshop, some responded that they felt they would be unable to contribute. Despite their work touching upon security, digital interactions and social media, the cultural and self-imposed research silos means that assumptions persist that some skillsets are inadequate or perhaps irrelevant for the topic of cyber security. This may be due to a narrow definition of cyber security that tends to solely focus on the technical aspects of the subject as opposed to also including its interplay with the social.

Finally, some participants brought up the issue of researcher safety in the region. Due to the nature of the sensitive topics they cover, some researchers felt they may be at risk of becoming targets themselves. This echoes a 2021 report from Access Now detailing examples of cases where cyber security researchers in Latin America had been persecuted by governments. Often this stems from a lack of technical understanding from the government, branding many of their activities such as the responsible disclosure of vulnerabilities as 'malicious'[3]. From our own discussions with other academics in the area, there are also concerns around personal safety when researching certain groups and spaces. In a region with

[1] See: https://www.uc.cl/noticias/conoce-el-nuevo-programa-uc-que-busca-cubrir-vacantes-de-empleo-en-ciencia-de-la-computacion/#:~:text=El%20Consejo%20Superior%20de%20la,a%20nivel%20nacional%20como%20internacional.

[2] See: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/programa-becas-especializacion-ciberseguridad

[3] See: https://www.accessnow.org/cms/assets/uploads/2021/08/persecution-infosec-latam-report.pdf

unfortunately high levels of organised crime, certain topics become difficult to research in person as they can put a researcher's life at risk.

Challenges in Policy Making

In a region with complex and existing security concerns, competing priorities becomes a challenge for cyber security policy making. When hunger, poverty, and crime are the everyday concerns of people, it is easy for cyber security to be relegated as an issue of secondary importance. As one participant noted, "cyber security is not a real problem *yet*", reflecting the view that as opposed to other issues, people are not '*getting hurt'* by cyber security issues at this moment. The lack of visceral and physical harms has made it harder for cyber security to be seen as a priority issue in the region.

Participants also noted that policymaking in the region has the tendency to be more reactive as opposed to forward thinking. That is to say, as issues emerge, cyber security policy is created, with few countries creating policy that intends to anticipate and prepare for the mitigation of potential threats. Laws and policies are created based on what has happened in the past and end up being more like ad hoc initiatives. As one participant noted, there is no "institutional or structural drive for cyber security". Furthermore, when policies are created, many countries draw from existing practices established in other states and contexts. Whilst following current best practices is not an issue per se, at times the policies do not match local realities or necessities. Importing cyber security concepts therefore can create challenges in the practice of cyber security if not adjusted to the country they are being implemented in.

Finally, this leads to the last challenge discussed in the workshop: implementation. Those countries that have tried to create policy and strategies around cyber security have often struggled to successfully implement them. At times this comes as a consequence of limited resources available, whilst other times the challenge emerges from implementing a policy that does not take into account cultural and societal factors.

2) POLITICAL CHANGE IN LATIN AMERICA

For the second part of the workshop, participants considered themes of political change in Latin America. This topic was broadly deliberated at two levels: the international level and the state level. It is interesting to note that though we expected conversations to centre around recent leadership changes in Latin America, we found that conversations expanded beyond this scope to include wider geopolitical considerations.

International Level

Relations to western states and institutions were repeatedly highlighted, with participants emphasising how western conceptualisations and practices of cyber security have influenced Latin American approaches. This report notes the duality between Latin American approaches to cyber security and relationships to the west in shaping such. On one hand partnerships with countries such as the United States, and the emulation of their policies, are seen as a benchmark for cyber security proficiency, yet on the other, there is a call to step away from Western approaches, allowing Latin American states to develop their own policies on cyber security independently.

To illustrate this, we can consider two examples from the discussions. Considering western relations and emulation of practice as an indicator of cyber capability, one participant suggested that Colombia has been able to present itself as a regional leader in cyber security. This presentation of regional ascendency was understood to be gained through knowledge transfer derived from a close relationship with the United States (though in reality Colombia's regional leadership in this area is up for debate). However, the development of capability, derived from collaborative projects with western states, is not necessarily guaranteed by such relationships. For instance, one individual drew attention to a four-year joint project between the United States of America, Canada, and Mexico to develop cyber security and critical infrastructure resilience. Considering issues of cyber security imposition and shared understandings, the participant asserted that the “project didn't get very far. The electrical grid was about all that could be agreed on. As soon as we had a change in leadership, projects would be dropped”. These comments reflect the difficulty of collaboration and the tensions derived from local realities which can undermine partnerships.

Further, participants drew attention to how western companies such as IBM and Microsoft have been increasingly driving political change in the cyber security space. In discussing these dynamics of technological development fostered by western private companies, issues of broader economic and geopolitical competition became important talking points. In particular that of China and Huawei. Drawing back to the influence of the west in relation to this issue, one participant noted that “the United States is telling them [Latin American states] to not use Huawei. But they are not given intelligence as to why they should not use it. They are expected to follow without questions asked”. Building on this, another participant suggested that the United States in recent times has very openly admitted to sharing intelligence with other states, and felt frustrated by this: “in Ukraine, a lot of intelligence was shared by the United States to put Ukraine in a better position and so Latin America wonders why the United States does not share any information with them?” Moreover, this participant noted, in light of the Snowden scandal, that to trust these western accounts was potentially problematic. Though these criticisms reflect valid frustrations, the reality of what information is shared publicly versus privately between Latin American and western states is unknown. Regarding Ukraine, intelligence sharing practices have been made very public, which might create the illusion that there is more information sharing, but we don't know for a fact if information is not being shared similarly behind closed doors with Latin American partners.

Participants often drew attention to issues of technological sovereignty and production, noting how Latin America is in a sense stuck between China and the western world. For instance, one contributor reflecting on the influence of Chinese telecommunications in Paraguay, highlighted how “the price of Chinese technology is much more accessible compared to European or American companies. Paraguay does not produce any technology ... they only use technology from other countries”. Multiple participants voiced similar views across the region, with one highlighting the strain on Latin American countries as they feel forced to take sides. Another suggested that "Latin America can feel pushed around – there is economic dependency with China but also familiarity with the United States". In this, contributors highlighted differences in motives between western dealings in Latin America, depicted as being underpinned by motivations of alliance and the maintenance of shared normative values, and China, who were characterised as being motivated by becoming "an economic partner". One participant suggested that "Latin America has been trying to have its own way", attempting to work both these relationships for their benefit.

Upon reflection there was little comment amongst participants on how political change within Latin America between neighbouring governments might drive certain forms of political change. For instance, the shift to left wing governments across the region might create opportunities for collaboration. Equally, such shifts might derive tensions and challenge existing structures of cooperation such as the Organisation of American States (OAS). This observation might reflect the limitations of the questions we raised and underlines a need to more directly address relations between states within the region.

State level

Internal histories of violent conflict and their impacts on digital infrastructures were a point of significant discussion. Amongst the most notable examples referencing such dynamics pertained to post-conflict Colombia. Participants highlighted how in the twenty-first century to interact and even engage as a citizen, access to digital infrastructure and services is often a necessity, as one individual put it "to become citizens you need infrastructure". In the case of Colombia, another highlighted how during the conflict in the rural regions in which FARC guerrillas operated, information communications infrastructure was destroyed to avoid government surveillance. Under conditions of conflict, such actions were deemed necessary to survive. Yet now, as this participant noted "citizens in rural zones of Colombia need cell phones to participate in society". This case reflects the broader conditional nature of security: what may be an act to secure under certain conditions, might create insecurity in others.

Of course, issues of conflict are not confined to history in much of Latin America. For instance, one participant highlighted that “some other countries are struggling, such as Mexico. They need to tackle crime, not cyber security”. There are limited resources and there is an opportunity cost to cyber security. Another participant considered how some countries such as Chile find it easier due to their already established institutions and infrastructures, “conversely, for others like Mexico and Brazil, it’s very expensive because they need to create entire institutions and bureaucracies”. Moreover, another suggested that “cyber security can be a scary word and can create more problems than solutions. The values that underlie this word are strong”. As one participant asserted, this “word is alien and foreign and it drives people away”. It is a term that fails to resonate with policy makers and is hard to perceive and understand.

Several participants noted concern around the impacts of populism on the cyber security agenda. One participant, commenting on the tenure of Andrés Manuel López Obrador in Mexico, suggested that his term has been detrimental to addressing cyber security issues, stating “back in 2017 cyber security was on the agenda, but now Mexico has an agenda with no strategy. [Now] there is no policy and just one person running cyber affairs”. Another, reflecting on the recent election of Gustavo Petro in Colombia and his policy of *Paz Total* (Total Peace) expressed “what does this mean for cyber security? We don't know”[4].

As a final aside, throughout this part of the workshop, participants stressed the importance and impacts of academia and the private sector as instigators of internal political change. One contributor suggested that in recent years it was “mostly university people pushing for cyber security to come back on the political agenda”. Another participant suggested that the private sector, in particular banking, has similarly advocated for greater focus on cyber security. Such comments illustrate how political change is driven by several groups and interests,

[4] Since this workshop Gustavo Petro has set out his national development plan for the next 4 years, that would create the National Agency for Digital Security and Spatial Affairs. Further details of how this will be implemented are yet to emerge.

reflecting the broader complexity of digital transformation emerging from the sheer number of competing interests. Moreover, these insights reflect how change does not necessarily emerge from top-down political processes, a theme that the next section of this report shall address.

Despite these movements and pressures emerging from the broader civil populace, there did seem to be a general agreement amongst participants that cyber will remain a relatively peripheral issue, at least in the short term. As one participant put it “in sum, there is an absence of a cyber security agenda in the Latin American region and the governments are not too concerned about it”.

3) EVERYDAY CYBER SECURITY PERSPECTIVES

A recurring theme which participants articulated as deserving greater attention is the everyday perspectives and experiences which communities in Latin America have of cybersecurity. 'Everyday' refers to the need to pay attention to the contextual histories and lived experiences of populations across the region. This enables an understanding of the reality of conflict, violence, crime, experiences of women, indigenous communities and marginalised groups on digital access and ultimately cyber security. One participant stated how, "there are many other risks to security in Latin America, and many other problems on top of this - so cyber security is part of a wide range of problems that need to be prioritised between". Further, participants of the workshop stressed, "A lot of the discussions around cyber security are from the global north without considering the context of Latin America". The call for Latin American perspectives is clear and this section introduces the key issues of conflict, grassroot approaches, and highlights some considerations around digital access.

Histories and Cycles of Conflict and Violence

From the conversations which arose there was a consensus that cyber security would be improved if research was culturally situated in order to understand the needs, priorities and concerns of local populations. Interesting discussions emerged throughout the workshop considering how physical security threats have translated into the digital. To expand upon this conversation, one participant brought up the concern of conflict and cyber continuing "cycles of violence" in Latin America. Attention therefore, should be paid to the "peripheral security agenda," that is, security issues of the everyday. The overlap of physical conflict and digital threats may not be unique to Latin America; however, the specific characteristics of the history and culture of each country and diverse community should be considered when developing cyber security policies. For example, discussions surrounding guerrilla warfare and the destruction of telecommunications infrastructure in rural Colombia, influence how security is perceived by communities impacted by violence, particularly concerning issues of surveillance. Such destruction also has a direct impact on digital access which will be discussed later in the report. This exemplifies how specific digital threats have been actuated by the historicity of everyday violence in the Colombian context.

Surveillance more broadly across Latin America is usually targeted at particular societal groups, “in which certain governments or companies buy software from other countries and use it to surveil different people in the Latin American region such as journalists, climate change activists, indigenous rights defenders, etc.” Targeted surveillance was then discussed in relation to privacy laws with exception being justified for anti-terrorism, anti-kidnapping, anti-extortion, and anti-drug trade by the governments. Participants brought targeted surveillance into discussion to how digital platforms can be exploited by drug cartels, another discussant continued, “Terrorist groups training in Mexico were discovered by footprints in cyberspace”. Again, bringing physical security issues into conversation with cyber in the context of Latin America.

Despite state specific discussions surrounding cyber security in relation to conflict and militarisation, one participant interestingly observed, “Latin America is the most peaceful region regarding interstate conflict and most violent in interpersonal conflict and/or violence. We have to shift focus more towards everyday violence and the use of technology to oppress people”. The conversation pointed to how cyber security could be enhanced by greater co-operation between Latin American states but also not focusing on interstate threats as the main concern in developing cyber policy, as this is a more predominant fear in the west. To further this again in the context of the everyday, the existence of policy is not enough and participants noted the disconnect between policy development and the enactment of such, “Governments see policy as resolving them of responsibility - it is then the people's job to behave securely”. As this report previously stressed, greater focus on integrating cyber security education into the everyday will improve cyber security awareness in Latin America.

Grassroots Approaches to Cyber Security

Conversations throughout the workshop highlighted the need for a grassroots approach to cyber security to understand the needs of the diverse communities across the region. Importantly, the discussions stressed how the experiences of marginalised groups are often overlooked. Yet, as the one participant noted, there has been, “an explosion in violence against women and the LGBTQ+ community in Latin America, worsening during the Covid-19 pandemic”.

Some participants therefore suggested that a greater focus on community focused, ground-up approaches to tackle issues such as gender-based violence may be needed. The prevalence of femicide is augmented with the use of digital tools. As one participant noted “attackers or abusers use media grooming, hate speech, dissemination of intimate images, cyber sexual harassment, [and the] usurpation of identity to gain more power over their victims”. The case of Juliana Campoverde in Ecuador was cited by the one participant as an instance where it is believed the murder investigation was hampered after “her Facebook account was hacked, and fake messages were implanted to prevent the people from knowing that she was indeed killed (and was not alive during that period)”. Despite femicide being a very real threat to women throughout Latin America there has been little to no cyber security research conducted in the region on this topic, and how digital technologies have been used by abusers to help them in their crimes. Apart from a few reports from civil society organisations, there is very little from the academic world that looks towards this space.

A closer look at the issues different communities in this region are encountering online suggests cyber security cannot solely remain focused at the national security level. To fully address sources of online insecurity, everyday online threats to marginalised communities should also be considered. Based upon the presentations and following discussions the definition of cyber security is different from Latin American perspectives and incorporates gender and physical violence.

Digital Access

Latin America is one of the most unequal regions in terms of access to digital tools and security. This could be observed even in the context of the workshop with one participant exclaiming frustration at his recurring connectivity issues, despite being in the capital city of Brazil in a building that was deemed to have 'good' internet. Digital access is linked to economic and infrastructural considerations and despite respondents agreeing that there needed to be greater digital expansion across Latin America, economic disparity of communities would only continue the digital divide.

A situated approach[5] to cyber security provides understanding to how populations experience digital access. For example, the predominance of instant messaging platforms, such as WhatsApp, was referred to by participants as a central tool of the internet. The prevalence of WhatsApp in Latin America is more so than in western contexts and allows for people to connect to services such as banking. WhatsApp is used for personal and business matters. Despite the usefulness of the platform, particularly as a way for people in remote places to connect, participants discussed potential scams. This tied into conversations surrounding education and awareness of cyber security and to what extent information was shared online in a more public way, "In Latin America we can confuse some platforms with the internet itself. The experience of going online is through social media apps, this is a challenge".

Discussing further the connections between situated, contextual histories and current concerns of digital access, we discussed how guerrilla attacks against key infrastructures in Colombia prevented rural communities from having connectivity. With poor connectivity comes poor security so here we call for greater conversations on specific restrictions to digital access in Latin America and on how this impacts cyber security.

[5] A situated approach is terminology used in HCI (Human Computer Interaction) studies which prioritises the cultural and societal context when conducting research.

LOOKING AHEAD

The workshop highlighted an apparent disconnect between the cyber security policy level, and everyday cyber security of citizens across various Latin American countries. This is one of the points the DSLA is interested in further exploring. States may be inclined to create policies that satisfy international standards and requirements but may do little to address the local realities and concerns of their own citizens. A closer look into why such a disconnect exists, as well as what issues may be overlooked, are both topics that we will continue to explore throughout future workshops. In this regard, calls from organisations like the Organisation for Economic Co-operation and Development (OECD) or civil society groups to adopt the language of "digital security" may help to include those wider concerns.

While no one is questioning the importance of the technical training of more individuals across the region to confront the new challenges emerging in cyberspace, a greater push is needed towards bringing down the silos that keep related research fields separate. The constant and widespread interaction between the digital and society means that cyber security does not occur in a vacuum. Every policy decision or design choice can have a real world impact on the people that make use of digital technologies. We must therefore continue facilitating the creation of bridges between different academic fields that can provide various perspectives, approaches, and solutions to the challenges we confront in this space.

Finally, the report is another example of the politics of cyber security. What is prioritised as an issue and *when* it is prioritised is a political choice. Discussions around cyber attacks, surveillance technologies, 5G equipment etc. are all issues that can provide a snapshot of a particular political moment and reflect the insecurities and preferences of different governments. As highlighted in the report, at times Latin American countries will opt for their own approaches to address these issues, whilst at others they will lean into their alliances with western states and draw from their best practices. Not all actors will react in the same way when confronted by the same challenges. For this reason, the historical, political, economic, and security context become an important aspect of cyber security research.

DSLA's Future Plans

Our report highlights the often understudied everyday aspects of cyber and digital security therefore, the next DSLA workshop will be about the everyday practices, narratives and definitions of 'digital security.' We wish to explore this from a grassroots and policy level and as always, we welcome input from both technical and non-technical perspectives.

We will share further details for this workshop via email and social media.

ACKNOWLEDGMENTS

We are very thankful to everyone who participated. Your insights and willingness to share your perspectives have been invaluable. We would also like to thank Marcos Tileria, Phil Sheriff, Sofía Celi, Carlos Solar, Benjamin Bencina, Mikaela Brough, MacGregor Cox, Oisín Phillips, and Faria Pitafi. Finally, we are very grateful for the support from the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London. Thank you for supporting us as we organised and carried out this workshop.

ABOUT THE AUTHORS

Sofia Liemann Escobar is a PhD candidate at the Centre for Doctoral Training in Cyber security for the Everyday at Royal Holloway, University of London. Her research looks at how cyber security is understood and practised in Colombia, with a particular interest in how cyber threats are conceptualised and constructed in the context of a country that is emerging from a decades-long conflict. Sofia's research interests rest more widely at the intersection of strategy, geopolitics, and cyber security. Prior to joining the CDT, Sofia completed a Master's degree in International Security at Sciences Po in Paris, and an undergraduate degree in War Studies at King's College London.	**James Barr** is a PhD student at the Centre for Doctoral Training in Cyber security for the Everyday at Royal Holloway University of London. His PhD explores the relationship between information technologies and conflict in Mexico, analysing how tools of communication and interconnectivity interact with and shape conflict. Prior to joining the CDT, James completed a BA in Politics and an MSc in Defence, Development and Diplomacy at Durham University with a focus on Lethal Autonomous Weapons Systems and their impacts on modern warfare.	**Jessica McClearn** is a PhD researcher at the Centre for Doctoral Training in Cyber security for the Everyday at Royal Holloway, UoL. Her research employs ethnographic methods to explore security in post-conflict contexts. Jessica's thesis will explore challenges to digital access and digital rights in Latin America. Recently she has also undertaken research in Lebanon, focusing on digital access and identity in the face of infrastructural collapse. This work will now take a LatAm focus, building on previous research she completed in Colombia. Prior to joining the CDT, Jessica completed her BA(Hons) in History and Social Anthropology at Queen's University Belfast and her MSc in International Management at Ulster University before living and working in New York for two years.

CONTACT DETAILS

Twitter: @DSLA_Research

Email: dsla.connect@gmail.com

Website: https://www.dslaresearch.org/