To: The Inter-American Committee against Terrorism (CICTE)
From: Roshie Xing
Subject: Addressing the Role of Information and Communication Technologies in Facilitating Violent Extremism

Introduction

The inception of the Internet and other Information and Communication Technologies (ICTs) have not only connected more individuals than ever, facilitating dialogue and highlighting injustice, but have provided a powerful platform to spread hatred and misinformation that have often resulted in physical violence.

Problem Statement/Background

Extremist groups have utilized a combination of online media sources, mainstream social media sites, and the Internet's more hidden spaces to spread propaganda to vulnerable individuals. Exclusive online interaction with similarly radicalized individuals creates environments akin to physical gangs, with these individuals growing desensitized to violence and increasingly willing to commit violent acts to further their particular cause. While the Islamic State's online recruitment tactics have been most publicized, this phenomenon is not isolated to a particular ideology or group. Neo-Nazis and the Far Right, Islamic fundamentalists, and left-wing groups like the National Liberation Army alike have exploited the far reaches of the Internet. Nor is it even exclusive to non-state actors. In Venezuela,[1] Brazil,[2] and Ecuador,[3] there has been evidence of social media "bots" being leveraged to artificially inflate the popularity of leaders, spread false information, and corrupt election integrity, sometimes with the backing of the state.

Governments have been slow to react to online radicalization pipelines–often not in deep corners of the Internet but on platforms such as Youtube–essentially allowing them free reign to flourish. This has been particularly dangerous during the COVID-19 pandemic, as many people are unemployed or out of school and as poverty and human suffering have grown dramatically. It is well documented that economic instability and general social and political turbulence result in greater susceptibility to messages placing blame on 'Others' for poor conditions.

Further complicating the issue is the thin boundary between freedom of expression and incitement to violence. In 2019, the OAS Special Rapporteur on Freedom of Expression made a joint statement with other international organizations recognizing the problems that arise with digital technologies, such as "terrorist recruitment and propaganda," but strongly warning against "undue legal

[1] Michelle Forelle et al., "Political Bots and the Manipulation of Public Opinion in Venezuela," *SSRN* (2015): https://dx.doi.org/10.2139/ssrn.2635800.

[2] *See* Julie Ricard and Juliano Medeiros, "Using misinformation as a political weapon: COVID-19 and Bolsonaro in Brazil," *Harvard Kennedy School Misinformation Review* 1, no. 3 (2020): https://misinforeview.hks.harvard.edu/article/using-misinformation-as-a-political-weapon-covid-19-and-bolsonaro-in-brazil/; Dan Arnaundo, "Computational Propaganda in Brazil: Social Bots during Elections," *Computational Propaganda Research Project* Working Paper 2017.8 (2017): https://blogs.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Brazil.pdf.

[3] Daniel Riofrio et al., "Tracking Elections: our experience during the presidential elections in Ecuador," *arXiv* 1807.06147 (2018): https://arxiv.org/abs/1807.06147.

restrictions on online expression."[4] This highlights not only the difficulty in addressing online radicalization, but the changing dimensions of modern security threats as a whole. Many of the tools traditionally used to counter violent extremism and preserve security–for example, surveillance and confiscation of arms–are at odds with other central rights like the freedom of thought and expression. Critically, the American Convention on Human Rights allows for the "imposition of liability" on this right when protecting national security or when it could incite violence motivated by "national, racial, or religious hatred." However, the Convention prevents "prior censorship" of such speech, and threats of ex post legal liability against certain speech could furthermore be abused to silence political opponents.[5]

In select cases, Member States have taken legal action against individuals who have used digital ICTs in relation to terrorist acts. Brazil, for example, arrested ten individuals in 2016 for promoting the Islamic State through social media and planning a terrorist attack through messaging apps; those involved had never met in person.[6] To date, however, there remains no general framework in Latin America for addressing how digital ICTs facilitate violent extremism, even as the groups exploiting them grow more adept in their usage. In contrast, organizations like the Organization for Security and Co-operation in Europe have worked with government, civil society, and business leaders to develop and disseminate best practices to combat the use of the Internet for terrorist purposes while protecting individual freedoms.[7]

CICTE has made moves to prioritize this issue, with CICTE's Executive Secretary Alison August Treppel stating last December that increasing reliance on the Internet due to the pandemic has "increased opportunities for the spread of...disinformation, and for online recruitment and radicalization."[8] In her remarks, Treppel underscored that virtual dialogues have shown that the Latin America and the Caribbean have "low capacity to counter online radicalization and violent extremist propaganda conducive to terrorism." Her statements stress the need for significant further research and policy action in addressing this pressing issue.

Perspectives/Theories

The OAS–and theories of international relations as a whole–has traditionally viewed security from the perspective of states struggling amongst themselves for power. Insecurity is framed as interstate conflict or even civil wars; both have nearly vanished in Latin America and the Caribbean. In contrast, non-state actors have contributed significantly to regional insecurity, resulting in the paradox of a region that is both "peaceful and violent."[9] The proliferation of drug trafficking and organized crime groups–

[4] Organization of American States Special Rapporteurship on Freedom of Expression, *Twentieth Anniversary of the Joint Declaration: Challenges to Freedom of Expression in the Next Decade*, https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1146&lID=1.

[5] Organization of American States, *American Convention on Human Rights*, B-32 (November 22, 1969).

[6] Lisandra Paraguassu and Anthony Boadle, "Brazil arrests 10 for 'amateur' terror plot against Olympics," *Reuters*, July 21, 2016, https://www.reuters.com/article/us-olympics-rio-security-operations/brazil-arrests-10-for-amateur-terror-plot-against-olympics-idUSKCN10121E.

[7] Organization for Security and Co-operation in Europe, *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach*, 36, 123-124.

[8] Alison August Treppel, Remarks by CICTE's Executive Secretary. *Virtual Open Briefing of the Counter-Terrorism Committee on "The Threat of Terrorism in Latin America and the Caribbean."* OAS. December 14, 2020.

[9] Rodrigo Tavares, *Security in South America: The Role of States and Regional Organizations* (Boulder: FirstForum Press, 2014), 1-6.

many of whom also take advantage of advances in ICT[10]–and violence from terrorist groups have supplanted territorial disputes. Consequently, there has been a push to conceptualize security at the individual level: the 'citizen security' perspective emphasizes the importance of individuals and law enforcement mutually cooperating to protect individual rights.[11] A more comprehensive perspective of security thus considers both traditional and human security threats, requiring the input of groups both higher and more localized than state governments.

Another consequence of malicious exploitation of digital ICTs is their threat to democracy. Arceneaux and Pion-Berlin have found that OAS mechanisms responding to democratic breakdown are best equipped for military threats and explicitly stolen elections, but willingness to respond to threats declines as a problem's ambiguity grows.[12] The spread of disinformation and stochastic terrorism driven by a few individuals radicalized online are such vague (and recent) threats as to not even be mentioned in their article; this likely explains some of the OAS' hesitancy to respond. Ultimately, taking decisive action against digital ICTs being used for extremist purposes is in both the rational and normative interest of states. The freedom of the Internet to communicate across vast geographical distances also increases the potential for violence spanning borders and broader regional destabilization. Volatile political environments have been worsened by social media bots spreading disinformation and radical messages, with the integrity of democratic elections being threatened and at worst, physical violence.[13]

Role of International Organizations

International organizations such as the OAS serve to facilitate cooperation and communication among member states. The digital components to violent extremism make it a borderless danger, necessitating intelligence and response sharing. Autarchical responses are insufficient, which places regional organizations in a position to provide expertise and coordinate action.[14] Presently, CICTE and other arms of the OAS have robust arrangements for security cooperation and information sharing, particularly on operations involving arms and drug trafficking.[15] These existing arrangements and similar ones through the United Nations Counter-Terrorism Committee and OSCE could be used to organize regional action countering the use of digital ICTs for extremist purposes. Further focus by CICTE on this issue would also prompt Member States to do the same, as most state plans to counter violent extremism have only focused on the digital realm in passing and on cybersecurity threats, if at all.

Conclusion

[10] Mark Berry, "Technology and organised crime in the smart city: an ethnographic study of the illicit drug trade," *City, Territory, and Architecture* 5 (2018): https://cityterritoryarchitecture.springeropen.com/articles/10.1186/s40410-018-0091-7.

[11] Robert Muggah, "The Rise of Citizen Security in Latin America and the Caribbean," *International Development Policy series*, no. 9 (2017): 4.

[12] Craig Arceneaux and David Pion-Berlin, "Issues, Threats, and Institutions: Explaining OAS Responses to Democratic Dilemmas in Latin America," *Latin American Politics and Society* 49, no. 2 (2007): 2, 10-11.

[13] Lara Jakes, "As Protests in South America Surged, So Did Russian Trolls on Twitter, U.S. Finds," *New York Times*, January 19, 2020, https://www.nytimes.com/2020/01/19/us/politics/south-america-russian-twitter.html.

[14] Tavares, 10.

[15] Sebastian Bitar and Tom Long, "International Security in Latin America," *Oxford Research Encyclopedia of Politics* (October 30, 2019).

It is imperative that as threats to member states grow increasingly transnational and complex, CICTE adjusts its strategies and focus as well. While states in the Americas have been relatively shielded from violent extremist attacks, particularly ones facilitated by digital ICTs, the region is not immune. There are already concerning reports of algorithms from sites like YouTube and Facebook drawing young people into the Far Right movement,[16] and other groups like Hezbollah have a history of online recruitment and subsequent terrorist attacks that could directly impact the security of Member States and their people.

Recommendations

In light of the urgency and nuances of the usage of digital ICTs for extremist purposes, the following recommendations are proposed:

First, to center youth voices in discussions on radicalization and security both at CICTE and at the state level.[17] Young people are frequently targets of online radicalization efforts, as they are more familiar with the Internet and are frequently dissatisfied with dwindling opportunities and the perception of large-scale government corruption. Consequently, they provide key insights on recognizing and countering such schemes.

Additionally, to increase information and strategy sharing on this new aspect of security and counter-terrorism among Member States. CICTE can facilitate this by creating a task force within its Inter-American Network on Counterterrorism dedicated to studying, monitoring, and countering online radicalization and the use of the digital ICTs for extremist purposes.

Finally, to emphasize community engagement in counter-extremism efforts. In the citizen security-based approach, community figures have been critical in identifying and engaging with individuals prone to using violence.[18] Increased investment into media and information literacy campaigns, especially in social atmospheres like schools, as well as encouraging monitoring and outreach on the part of community leaders could contribute to countering disinformation and violent rhetoric online.

[16] Max Fisher and Amanda Taub, "How YouTube Radicalized Brazil," *New York Times*, August 11, 2019, https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html.

[17] An example of one such initiative is the World Bank and Government of Tajikistan's joint report: *Strengthening Youth Resilience to Radicalization: Evidence from Tajikistan* (2020): https://www.worldbank.org/en/region/eca/publication/strengthening-youth-resilience-to-radicalization-evidence-from-tajikistan.

[18] Muggah, 11.