Global Security Review

Volume 2 *Strategic Competition: Russian and Chinese Influence in Latin American and the Caribbean* Article 1

January 2022

Strategic Competition: Russian and Chinese Influence in Latin America and the Caribbean

JACK D GORDON INSTITUTE FOR PUBLIC POLICY

GLOBAL SECURITY REVIEW

GSR

VOLUME 2 | JANUARY 2022

STRATEGIC COMPETITION

RUSSIAN AND CHINESE INFLUENCE IN LATIN AMERICA AND THE CARIBBEAN

FIU Steven J. Green School of International & Public Affairs

ISBN
9781234567897

Page intentionally left blank

GLOBAL SECURITY REVIEW

Global Security Review is the flagship journal of the Jack D. Gordon Institute for Public Policy at Florida International University's Steven J. Green School of International and Public Affairs. This journal seeks to publish pieces by leading academics, policy analysts, and practitioners on important security issues in the twenty-first century. Each issue deals with a particular topic related to global security. The articles seek to be innovative and bridge the academic policy divide.

LETTER FROM THE DIRECTOR

The Jack D. Gordon Institute for Public Policy, which is part of the Steven J. Green School of International and Public Affairs (SIPA) at Florida International University (FIU), is honored to publish the second issue of *Global Security Review* (GSR). GSR represents our institute's ongoing effort to bridge the divide between academia and the policy world and to increase public understanding of the most critical national security challenges. The first issue addressed a wide range of threats that impact national security, from the late Robert Jervis' article on global terrorism to pieces on U.S. energy security, Plan Colombia, terrorism in the Caribbean, and the growing cyber threats. This issue focuses on strategic competition in Latin America and the Caribbean and the geo-political implications.

The global environment of the Twenty-First Century continues to become more politically, culturally, and technologically complex with the increasing connectiveness of the world, growth within the cyber domain, and the importance of the information environment in controlling narratives. A rising China, a recalcitrant Russia, and a growing number of proxies challenge western values and U.S. hegemony in the world, particularly in Latin America. Using a variety of military and economic tools, as well as disinformation and soft power, China and Russia create strategic ambiguity that reduces recognition of threats and appropriate responses by partner nations. Lines between war and peace are blurred, leading to a new paradigm of strategic competition.

The first article by Hal Brands and Ryan Berg provides an overview of strategic competition in the Western Hemisphere, adding historical and political context to its evolution since the Monroe Doctrine. It provides principles for an appropriate U.S. response. Margaret Myers follows with an insightful look at China's COVID-19 Diplomacy in the region, to include its objectives and methods that are intended to reinforce regional ties and advance commercial and policy interests. Vladimir Rouvinski pivots to another great-power rival, Russia, and its return to the Western Hemisphere. He explains Russia's view of its right to advance special interests in neighboring, former Soviet states and how this drives Russian motivations within Latin America and the Caribbean, as well as its efforts to control the narrative in the information environment. Furthermore, many environmental, economic, political, security, and health factors have driven significant migration throughout the world in recent years. Betilde Muñoz-Pogossian and Diego Chaves-González explore the relationship between natural disasters, internal displacement, and violence as drivers of Central American migration. As an increasing number of state and non-state actors conduct a variety of cyber operations, Louise Marie Hurel looks beyond "great powers" in her article examining how Latin America views cyber operations and norms. Finally, Marcus Boyd and Samuel Henkin address the growing threat of transnational organized crime, and their global scope, institutionalized violence, and impact on the global economy.

In conclusion, we hope that you enjoy our second issue of *Global Security Review*. GSR will be published annually and include articles from leading scholars and practitioners that address the most pressing national security issues. FIU and the Gordon Institute will continue hosting conferences and workshops and publishing policy papers, reports, books, and articles on these topics, and will include this content in FIU's Security Research Hub. The Security Research Hub is a centralized, open-source community that supports collaboration and shared understanding on security topics by leveraging subject matter experts from across academia, civil society, government, and private industry.

Brian Fonseca

DIRECTOR | JACK D. GORDON INSTITUTE FOR PUBLIC POLICY

TABLE OF CONTENTS

Ryan C. Berg & Hal Brands

[1] This article is taken from a larger report published by Ryan C. Berg and Hal Brands titled "The Return of Geopolitics: Latin America and the Caribbean in an Era of Great-Power Rivalry". The full publication can be found at www.gordoninstitute.fiu.edu/research/publications.

With the advent of the Biden administration, it has become clear that the idea of focusing U.S. strategy on "great-power competition" enjoys widespread bipartisan support. American statecraft is increasingly directed at the threats posed by powerful state rivals—especially China—as opposed to Salafi-Jihadist extremists and other non-state actors.[2]

Yet geopolitical rivalry is not simply something that happens "over there," in the Indo-Pacific, Europe, and the Middle East. It also happens "over here"—within the Western Hemisphere.

Just as geopolitical competition is more the norm than the exception for the United States, historically America has faced recurring threats from major-power rivals operating in Latin America. This pattern is repeating itself today, as the countries—China, Russia, and to a lesser extent, Iran—with which the United States is competing in overseas regions are, in turn, competing with the United States in its shared neighborhood. These challenges have not yet risen to the level of the Cold War-era threat posed by the Soviet-Cuban alliance or even the Nazi presence in many Latin American countries prior to World War II. But they are gradually calling core American strategic interests in Latin America into question.

For roughly 200 years, the core American interest in the region has been strategic denial—preventing powerful rivals from achieving strategic footholds in Latin America or otherwise significantly impairing U.S. influence and security in the region. The nature and severity of the challenges to that objective have varied over time, as have the urgency and methods of the American response. As the United States enters a new period of geopolitical rivalry, it must update its understanding of strategic denial to fit the facts on the ground.

The tradition of strategic denial

The essential thrust of U.S. policy in the Western Hemisphere has thus been strategic denial vis-à-vis other great powers. American officials have sought to prevent major rivals from developing regional footholds from which they can menace, distract, or otherwise undercut the strategic interests of the United States. There has also been a persistent, if not always consistent, ideological component to strategic denial—a belief that non-democratic political systems in Latin America and the Caribbean constitute a conduit through which malign actors can exert their influence. "It is impossible that the allied powers should extend their political system to any portion" of the Americas, stated James Monroe in his eponymous doctrine, "without endangering our peace and happiness."

Yet if the basic objective of strategic denial has endured over time, the manifestations and targets of that policy have repeatedly shifted. The Monroe Doctrine warned against a restoration of formal European colonial empires in Latin America; the "political system" it sought to exclude from the hemisphere was monarchy. Although John Quincy Adams prevailed on Monroe to issue that statement as a unilateral declaration rather than "come in as a cock-boat in the wake of the British man-of-war," it was London—which had its own policy of strategic denial vis-à-vis its European rivals—whose navy enforced the edict for most of the 19th century. The United States, for its part, spent much of this period trying to prevent, not always successfully, the expansion of European influence in Latin America rather than liquidating it where it remained.

This posture changed in response to growing American power and shifting international threats. In 1898, the United States defeated—for the first time since the American Revolution—a European power in a major military conflict and thereby banished Spain from the hemisphere. During the 1890s and early 1900s, America used various forms of coercive diplomacy to reduce a distracted United Kingdom's influence around the Caribbean basin and gain exclusive control over the routes for an isthmian canal. Meanwhile, concerns that internal instability and financial insolvency might invite European interposition elicited the Roosevelt Corollary, which established a tradition of "protective imperialism"—of Washington intervening in troubled Caribbean countries so that hostile actors would not have a pretext to do so. This theory of strategic denial paved the way for multiple American interventions—in the Dominican Republic, Haiti, Nicaragua, even Mexico—in the subsequent decades.

That heavy-handedness provoked blowback, however, and in the Franklin Delano Roosevelt era, strategic denial took on yet another form—this time under the moniker of a "good neighbor policy." FDR would end lingering U.S. occupations, hoping that a less invasive presence focused more on economic ties and de-emphasizing a military dimension of strategic denial—combined with the steady hand of friendly dictators—would better consolidate the hemisphere against the

growing fascist threat. At the Havana Conference in 1940, the United States announced, in the guise of a multilateral declaration, that it would enforce the Monroe Doctrine against any extra-hemispheric power that violated the territorial or political sovereignty of a Western Hemisphere state. The fear persisted, particularly after the fall of France, that Nazi Germany would use subversion, economic coercion, or even direct aggression to turn South American or Central American countries into platforms to threaten the United States.[3] In response, Washington used various methods, from good intelligence work to blunt diplomatic pressure, to limit German influence in the region and eventually bring Latin American and Caribbean governments into World War II on the side of the Grand Alliance.

During the Cold War, the target of strategic denial was Moscow; the danger was that local communists would take power, through peaceful or violent means, and turn their countries into beachheads for Soviet military and political influence. As Castro's revolution in Cuba showed, a Soviet presence in the Caribbean would endanger American sea lines of communication and expose major gaps in the country's air defenses. It would be a launching point and logistical, financial, and training hub for other burning insurgencies in the region. A United States consumed with fighting communist regimes and revolutionaries close to home would, in turn, find it far more difficult to concentrate its energies on checking Soviet influence in Europe, the Middle East, or Asia. It might even find its physical security endangered. It was this prospect that led Jeane Kirkpatrick to declare, in the 1980s, that Central America was "the most important region in the world."[4]

The United States used the full panoply of tools—economic development programs, military coups, covert action, and direct military intervention—to fight the expansion of Soviet and Cuban influence. In some cases, it sought to promote democracy and economic reform as antidotes to revolution; in others, it partnered with conservative or downright reactionary Latin American regimes such as the Brazilian military dictatorship to bludgeon leftist movements. But by the 1980s, Washington was more decisively moving toward a strategy that employed democratization as a tool of strategic denial, by establishing legitimate regimes that would be less vulnerable to challenges by Marxist insurgents.

Within another few years, the Cold War had ended, and the threat of alien ideologies and extra-hemispheric power faded more fully than ever before. They did not, however, disappear for good.

U.S. Blind spots and the Latin America paradox

The post-Cold War era also revived another, and less salubrious, tradition in U.S. policy—the Latin America paradox. That paradox resides in the fact that Latin America is perhaps the most important region for the United States, in the sense that pervasive insecurity or danger there could pose a more direct threat to America than equivalent disorder in any other region. The Mexican Revolution, for example, elicited not one but two U.S. military interventions for just this reason. But Latin America has traditionally received considerably less foreign policy attention than other regions because American influence there—while periodically challenged—has long been so preeminent.

Since the 1990s, this blind spot has been exacerbated by several other factors. First, although there have been major security challenges in the region, most have taken the form of drug-related violence and out-of-control criminality—domestic challenges often viewed as law enforcement matters that lack an obvious geopolitical salience. Compare, for instance, the remarkably scant attention that ongoing state failure and rampant violence in Mexico have received over the last fifteen years to the attention those phenomena would have received had it been caused by a Communist insurgency with links to the Kremlin during the Cold War. "Law enforcement problems" are, by their nature, unsexy in the foreign policy world.

Second, the largely democratic nature—or perhaps the democratic patina—of the region has masked the severity of underlying challenges. Since the early 1990s, the vast majority of Latin American and Caribbean governments have been democracies, in the sense that they have regular, contested elections. After Mexico's transition in 2000, Cuba was the only fully authoritarian regime in the hemisphere. Yet the existence of democratic procedures, consolidated in regional diplomatic accords such as the Inter-American Democratic Charter, has obscured concerning levels of political backsliding in countries from Central America to the Southern Cone, in addition to the emergence of violently repressive authoritarianism in Venezuela. It has also dulled the U.S. response to the creeping accumulation of extra-hemispheric influence in hemispheric affairs, in many cases through the exact same countries experiencing a rapid decline in the quality of democratic governance.

Finally, blind spots in Latin America have been exacerbated by the intensity and number of challenges the United States has confronted elsewhere. The 9/11 attacks led to a heightened focus on Colombia, because

the guerrilla insurgency there could be viewed through a counter-terrorism prism. But in most cases, the war on terror diverted focus from the region. More recently, American resources and attention have been consumed by a remarkably full foreign policy agenda—ongoing instability in the Middle East and Africa, including a chaotic withdrawal from Afghanistan, a resurgent and revisionist Russia, periodic North Korean nuclear crises, the rise of China as a regional and increasingly global power, along with the pressing problems posed by climate change, pandemics, and other transnational challenges. Even as the situation has deteriorated in Latin America and the Caribbean, the region has had to compete with a remarkably crowded and challenging foreign policy panorama. And amid the resulting distraction, several state actors are once again vying for influence in the Western Hemisphere.

Contemporary challenges—China

The primary threat to American interests in Latin America comes from China, both because Beijing is the greatest global challenge for American statecraft and because its presence in the Western Hemisphere is multifaceted and widespread. As part of a strategy to increase its own influence and options in the region while creating potential problems for the United States close to home, China engages governments and supports political models in the region that are hostile to American interests, while also courting traditional U.S. allies.

The leading edge of China's involvement in the Western Hemisphere is economic. For roughly a generation, Beijing has been leveraging its massive domestic market and vast financial resources to draw countries in the region closer and pull them away from Washington. China is now the region's second-largest trade partner behind the United States. While the United States still enjoys a comfortable lead in this metric, its advantage has been eroding since the turn of the century. Between 2000 and 2018, the percentage of Latin American exports going to the United States dropped from 58 to 43 percent while it increased from 1.1. to 12.4 percent with respect to China. In fact, discounting Mexico, China already surpassed the United States as the largest destination country for the region's exports.[5] Importantly, China has linked itself closely with the largest economic power in the Western Hemisphere outside the United States—Brazil. Beijing has become Brazil's most important commercial partner, doubling in size compared to the Brazil-U.S. commercial relationship.[6]

China also uses its Belt and Road Initiative (BRI) to project its economic power and improve its geopolitical position. Since its launch in 2013, BRI has become one of the most ambitious global development programs in history. According to Chinese officials, its rapid growth in Latin America represents a "natural extension of the 21st Century Maritime Silk Road."[7] Thus far, 18 countries in Latin America have signed on to BRI—including some of the most prosperous countries in the region, such as Chile.[8]

While BRI is attractive to recipient nations because it purports to address real infrastructure needs and other development shortfalls, the resulting Chinese economic leverage can become a means of extracting political concessions. For example, when Sri Lanka fell into arrears on the loans it had taken from China (loans other sources had declined due to risk), it was left with no other option than to turn over the Hambantota Port, plus thousands of acres of land surrounding it, to the Chinese for 99 years.[9] China may use the same tactic to obtain strategic footholds in the Western Hemisphere, perhaps taking advantage of high debt burdens owed by small island nations in the Caribbean. Regionwide, the acute debt crisis that could be the legacy of COVID-19 may provide further openings for predatory Chinese finance throughout the region.

Technology is another weapon of Chinese influence in Latin America. Huawei, the Chinese telecommunications company, is one of the market leaders of mobile devices in the Hemisphere. Huawei is also a top contender for the upcoming 5G auctions in Brazil, Chile, and Mexico. Although the company repeatedly claims its independence from the Chinese state, the company possesses an intentionally opaque corporate structure, and Chinese law requires that Chinese entities "support, assist and cooperate with state intelligence work."[10] Accordingly, the U.S. is attempting to persuade countries in the Hemisphere to reconsider adopting Chinese equipment. American officials have already warned countries that adopting Huawei technology would make information sharing and collaboration with the United States difficult if not impossible.[11] U.S. lawmakers have also introduced legislation to restrict intelligence sharing with countries that use Huawei equipment in their 5G networks.[12] Additionally, Washington has offered economic incentives to try to tip the scale away from Chinese companies. For example, the U.S. offered Brazil, an erstwhile member of the "Clean Network," generous terms of finance to purchase 5G equipment from other (non-American) sources.[13]

Although Chinese engagement in Latin America is primarily economic in nature, military collaboration is a growing aspect of Chinese activity in the region. Arms sales, military training, and technical military support allow the Chinese to build key strategic relationships with the armed forces of countries in the United States'

shared neighborhood. The Chinese have sold equipment to military and police forces from countries historically opposed to the United States—such as Venezuela and Cuba—as well as close American partners like Colombia and Chile. The People's Liberation Army (PLA) maintains a growing presence in the region through training and visits, which permits it greater familiarity with countries' operational frameworks and preparedness, as well as their strategic doctrine.[14] China has also focused on ongoing training of the region's military officers at PRC institutions of military education, which should familiarize and educate the upper brass in Chinese military doctrine.[15]

More ominously, the PLA is rapidly building new dual-use infrastructure or acquiring access to existing dual-use infrastructure that can enhance its military capabilities in the region. For example, China has several dozen agreements to build or expand deep-water ports in the region, and it constructed a space station operated by the PLA in Neuquén Province, Argentina, without Argentinian oversight. While the Chinese claim that this installation is for peaceful space exploration, the base has obvious dual-use potential as a tool for espionage, and China does not permit the Argentines to come near the facility.[16] Quite ominously, China has signed another agreement for a similar facility in Santa Cruz Province; the strategic importance cannot be overstated, as Santa Cruz lies just above the Strait of Magellan, a major maritime chokepoint.[17] Likewise, China's growing partnership with Panama may eventually result in preferential access to the Panama Canal, facilitating the movement of goods and people in and out of the Hemisphere and inflicting a symbolic as well as strategic blow to the United States. Two-thirds of all ships transiting to and from the U.S. pass through the Panama Canal.[18]

China is doing more than just developing its economic and military presence in the region. The Chinese are also applying soft power capabilities to make their burgeoning influence seem less threatening.[19] Vaccine diplomacy is China's latest soft power play in the Hemisphere. Even though the Chinese government's attempt to cover up the outbreak of COVID-19 assisted the virus in its spread worldwide, China is now repairing (and even enhancing) its reputation by providing personal protective equipment (PPE) and vaccines against the virus to Latin American countries. Even Brazil, whose president is rhetorically quite hostile to China, has been left with no other option than to acquire China's Sinovac vaccine, lest Brazil be without vaccine.[20] And although Chinese officials claim that Beijing "never seeks geopolitical goals and economic interests" in exchange for vaccines, this does not seem to be the case.[21] Shortly after initial talks on the possibility of Brazil receiving vaccines from China, Brazil announced the rules for its 5G auction, which allowed Huawei to participate—reversing earlier comments by government officials that seemed to favor barring the Chinese company and committing Brazil to the United States' "Clean Network" initiative.[22] China also slowed its vaccine delivery schedule of vaccines after a diplomatic spat between the president's son, Federal Deputy Eduardo Bolsonaro, and Chinese ambassador to Brazil, Yang Wanming.

Contemporary challenges—Russia

Russia is a secondary threat to American interests in Latin America, as overall, Russian power is more limited and less multidimensional than China's. Nonetheless, since the early 2000s Russia has publicly expressed interest in expanding its presence in the region. Moscow's 2016 Foreign Policy Concept of the Russian Federation proclaims: "Russia remains committed to the comprehensive strengthening of relations with the Latin American and Caribbean States taking into account the growing role of this region in global affairs."[23]

Most evidence suggests that Russia views its presence in Latin America primarily as a modest rejoinder to American influence in Russia's near abroad—a way of gaining strategic leverage on the United States and diverting its geopolitical energies. Contrary to China's more robust efforts, however, Russia has circumscribed its activity and sought to expand its influence in the Western Hemisphere primarily with countries that have been historically opposed to the United States and with regimes of an illiberal nature. (Unlike China, it has little to offer healthier, more politically stable and liberal states.) Russia has been actively involved with the grouping of states in the Bolivarian Alliance for the Peoples of Our America (ALBA)—most notably Venezuela, Cuba, and Nicaragua.

Perhaps the primary way Russia supports Latin America's illiberal regimes is with military assistance, through arms sales, technical support, and military training and visits.[24] Nicaragua serves as a prominent example. Russia provides practically all of Nicaragua's armaments, many of which became key instruments of terror in Nicaragua's 2018 uprising and the Ortega regime's brutal suppression of it. (For instance, Dragunov sniper rifles sold to the Nicaraguan Army ended up in the hands of well-trained paramilitary groups that used them to fire indiscriminately at protestors.) In 2014, the Russian military opened a training facility in Nicaragua, where numerous Russian military personnel are stationed—purportedly for joint military exercises and anti-trafficking efforts, but possibly to aid President

Daniel Ortega's efforts to suppress political opposition. A year later, Nicaragua permitted Russian warships access to Nicaraguan ports and, in 2017, Nicaragua agreed to allow Russia to build a Global Navigation Satellite System (GLONASS) station—conveniently stationed in proximity to the U.S. Embassy in Managua—that is likely used for intelligence gathering.[25] Russia has grown its influence in Nicaragua as the Ortega regime's plans to install a family dynasty have become clear. Most recently, it has revealed an agreement to share cyber tools with Nicaragua to bolster regime resilience and potentially spy on opposition figures.[26]

Disinformation and propaganda are also powerful and fine-tuned Russian tools. They allow Russia to manipulate public opinion and spread anti-western sentiment throughout the region—especially toward the United States. Russian state-owned news outlets have expanded their reach in Latin America with Spanish television and news networks such as Russia Today en Español and Sputnik Mundo. According to its website, Russia Today en Español reaches 18 million people a week in ten different Latin American countries and has more than 3 billion total views on its YouTube channel.[27] As with Chinese outlets, regional news organizations often republish many of these stories.

In the economic realm, Russian trade with the Hemisphere is not substantial. Nevertheless, Russia plays a significant role in providing governments in the region financial support and helping them circumvent sanctions. Like China, Russia provides loans to friendly regimes with few strings attached and is flexible with repayment, including payment in-kind (as it does with Venezuelan crude). In 2015, Russia extended a $1.5 billion loan to Cuba (the largest since the fall of the Soviet Union) with a generous interest rate to build large power plants on the island.[28] A mere year earlier, Russia excused 90% of Cuba's Soviet-era debt totaling over $30 billion.[29]

Russian assistance with sanctions evasion is critical for the survival of certain countries in the Hemisphere, notably Venezuela. For example, after the U.S. imposed sanctions on Venezuela's state-owned oil company, Petróleos de Venezuela (PDVSA), Russia's state-owned oil company, Rosneft continued to do business with PDVSA. (The U.S. later designated Rosneft Trading and TNK Trading, the Swiss-based Russian subsidiaries in question in these endeavors, for sanctions.) Russia also appears to have been quietly involved with Venezuela's effort to design a national cryptocurrency, called the Petro, to help the Maduro regime avoid international sanctions.[30] While the Petro has been unsuccessful due to bureaucratic incompetency and lack of domestic and international enthusiasm, Russia will continue to aid its beleaguered ally in the effort to evade American economic leverage.[31]

Principles for a U.S. Response

Geopolitics are back in Latin America, with great-power rivals seeking to use the Western Hemisphere as a point of strategic leverage against the United States. The United States will need a long-term, strategic response. There appears to be some prospect that the region will receive greater relative priority in U.S. policy: The Biden administration implicitly ranked the Western Hemisphere above the Middle East in its Interim National Security Strategic Guidance. Nonetheless, short of a major crisis, there is little likelihood that the absolute level of resources the region receives will increase dramatically in the near-term. With this in mind, we offer a few basic principles for a strategic response to the deterioration of American influence in the region, one that is mindful of resource constraints and the limits of what Washington can achieve within them.

First, *track extra-hemispheric influence more systematically.* The U.S. government will need a more complete cataloguing of great-power activity and presence in its shared neighborhood, as one recent bill before the U.S. Congress requires.[32] Just as important will be establishing qualitative and quantitative metrics to monitor and evaluate the presence of its geopolitical rivals in the Western Hemisphere. Lacking such metrics, policymaking will continue to be conducted on an ad-hoc basis. Given the multi-dimensional nature of great power competition illuminated in this report, developing such measurements is not a straightforward endeavor. However, proximity and threat level (regarding both military and economic challenges to the United States) should be guiding principles in this effort to establish thresholds for greater action. In particular, the U.S. would be wise to systematically monitor the transfer of dual-use infrastructure and technology to the region and determine at what point such transfers would cross a critical threshold, presenting a point of significant strategic leverage against core American interests.[33]

Second, *track vulnerabilities as well as strengths.* The expansion of Chinese and Russian influence in Latin American and the Caribbean has not always been a popular phenomenon. Industries and enterprises have been hurt by economic competition; support for corrupt and illiberal regimes has tarnished the reputation of China and Russia with some local populations. Heavy-handed vaccine diplomacy (with substandard quality vaccines and defective personal protective equipment to boot) could create further vulnerabilities for China

in particular (and Russia, to a lesser extent). Studying which aspects of these countries' regional presence create diplomatic or soft-power vulnerabilities is a starting point for developing a more competitive response.

Third, *engage on security issues of greatest concern to local governments and peoples.* The United States must present itself as the preferred partner to help countries in the Western Hemisphere address their security concerns. Washington has had some success in this regard in the past, with wide-ranging security assistance programs such as Plan Colombia and the US-Mexico Merida Initiative. In other cases, however, American policy initiatives have focused on issues—such as curbing migration—of comparatively lower concern to regional partners. To compete effectively, the United States must also prioritize the preferred security challenges of its partners—and understand that those challenges are quickly shifting. The burgeoning threat represented by China's highly subsidized illegal, unregulated, and unreported (IUU) fishing activities in sensitive ecological waters off the Pacific Coast of South America is but one example of the rapidly evolving nature of the region's security environment.[34]

Fourth, *counter the authoritarian playbook.* While the presence of great-power rivals has often exacerbated political instability and furthered democratic backsliding in Latin America and the Caribbean, the truth is that preexisting political tensions, endemic corruption, and a poor record of governance in many countries throughout the region leaves them vulnerable to Chinese and Russian influence. In the domestic context, there is a well-worn playbook that leads to authoritarianism, which includes electoral reengineering, suffocation of civil society and the corruption of the media's independence, and the weakening of political opposition and political institutions, capped off by the politicization of judiciaries and military and police forces. Sometimes, leaders following the authoritarian playbook even consolidate their gains by amending or rewriting their country's constitution.[35] Fortunately, the tools inherent in the Inter-American Democratic Charter can help to sound a powerful tocsin against democratic backsliding and the authoritarian playbook. Maintaining the largely democratic nature of the region and focusing on improving the quality of governance and political institutions can both reduce the openings for the authoritarian playbook and limit opportunities for great-power rivals to use backsliding democracies and nascent autocracies as convenient entry points into America's shared neighborhood.

Fifth, *don't make it all about China.* There is no question that American interest in Latin America and the Caribbean rises when perceptions of extra-hemispheric threats become more acute. But just as the United States sometimes misfired, during the early Cold War, by focusing excessively on the dangers of communism—as opposed to aspirations for local political and economic progress—in the developing regions, it is a mistake to convey the impression that Washington cares about the Western Hemisphere only because of the Chinese or Russian threats. Similarly, while there are times when public critiques of Chinese policies by U.S. officials are entirely warranted, another lesson of the Cold War is that those critiques are often more effective when delivered by friendly local actors rather than by the United States itself.

Sixth, *emphasize cost-effective means of competition.* When resources are relatively scarce, the United States will need to find ways of increasing the bang it receives for each buck. There are a variety of possibilities. IMET (International Military Education and Training) initiatives are an inexpensive means of building relationships with the next generation of Latin American military leaders—relationships that the United States is in growing danger of not having in the future. Visits by high-level American officials that have not historically received much attention from the United States, can also play an outsized role in warding off rivals' influence. Showing up does matter: Taiwan, for example, has used this sort of approach to maintain is diplomatic toehold in the region.

Seventh, *leverage non-governmental advantages.* Great-power competition encompasses more than just state action. This is where the United States can leverage asymmetric advantages. The United States has deep cultural, political, and historical ties with its southern neighbors, exemplified by the large number of immigrants and diaspora groups in the United States who hail from the region. These immigrants and their decedents have a deep sense of patriotism that rivals (and often surpasses) those of native-born U.S. citizens.[36] Facilitating people-to-people diplomacy—by relaxing travel restrictions, expanding trade links, or professional development programs through public-private partnerships—can be a cost-efficient way for the United States to strengthen its hemispheric relationships and limit the influence of its great-power rivals.

Eighth, *understand that you ultimately get what you pay for*. Most analyses of deteriorating U.S. influence in Latin America and the Caribbean focus on the resource-poor approach Washington has taken to the region over the past 30 years, and call for a more holistic, better-supported strategy. We have no reason to differ from this basic recommendation.

Most, although not all, countries in Latin America and the Caribbean still see the United States as a preferred partner on many issues of concern and regret that there are not greater opportunities to engage with Washington on these issues. Defending American interests in the region will indeed require a whole-of-government effort to provide countries in Latin America and the Caribbean with alternatives to economic, diplomatic, and military reliance on extra-hemispheric rivals, in areas such as investment, 5G telecommunications, strengthening governance, pushing for greater transparency (in development and other projects), and highlighting the predatory aspects of China's advance while not appearing to block countries from taking advantage of the trade and investment resources Beijing can offer. In the coming years, the United States will likely need to pursue competition on a strictly limited budget. But if it does not make greater preventive investments in the region now, it may once again experience the historical pattern of having to make far greater compensatory investments once key tipping points have been reached and emerging strategic challenges have become impossible to ignore.

REFERENCES

[1]This article is taken from a larger report published by Ryan C. Berg and Hal Brands titled "The Return of Geopolitics: Latin America and the Caribbean in an Era of Great-Power Rivalry". The full publication can be found at www.gordoninstitute.fiu.edu/research/publications.

[2] See National Security Strategy of the United States of America, December 2017; and Interim National Security Strategic Guidance, March 2021.

[3] Max Paul Friedman, Nazis and Good Neighbors: The United States Campaign against the Germans of Latin America in World War II (Cambridge: Cambridge University Press, 2003).

[4] See Hal Brands, Latin America's Cold War (Cambridge: Harvard University Press, 2010).

[5] Claudia Trevisan, "Trade, Investment, Technology, and Training are China's Tools to Influence Latin America," February 2, 2021, Council on Foreign Relations and Brazilian Center for International Relations, https://cdn.cfr.org/sites/default/files/pdf/trevisan-cfr-cebri-paper_0.pdf.

6 Guilherme Venaglia, "Brasil e China: O que está em jogo na relação com nosso maior parceiro commercial," CNN Brasil, December 12, 2020, https://www.cnnbrasil.com.br/business/2020/12/12/brasil-e-china-o-que-esta-em-jogo-na-relacao-com-nosso-maior-parceiro-comercial.

[7] Jacob J. Lew et al., "China's Belt and Road: Implication for the United States," Council on Foreign Relations, March 2021, https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/; June Teufel Dreyer, "The Belt, the Road, and Latin America," Foreign Policy Research Institute, January 16, 2019, https://www.fpri.org/article/2019/01/the-belt-the-road-and-latin-america/

[8] "Countries of the Belt and Road Initiative (BRI)," Green Belt and Road Initiative Center, last modified January 2021, https://green-bri.org/countries-of-the-belt-and-road-initiative-bri/.

[9] Maria Abi-Habib, "How China Got Sri Lanka to Cough Up a Port," New York Times, June 25, 2018, https://www.nytimes.com/2018/06/25/world/asia/china-sri-lanka-port.html.

[10] Arjun Kharpal, "Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice." CNBC, March 4, 2019, https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

[11] Lesley Wroughton and Gergely Szakacs, "Pompeo warns allies Huawei presence complicates partnership with U.S.," Reuters, February 10, 2019, https://www.reuters.com/article/us-usa-pompeo-hungary/pompeo-warns-allies-huawei-presence-complicates-partnership-with-u-s-idUSKCN1Q0007.

[12] Arjun Kharpal, "Senator seeks ban on US sharing intelligence with countries using Huawei 5G gear," CNBC, January 9, 2020, https://www.cnbc.com/2020/01/09/us-lawmaker-seeks-intelligence-sharing-ban-with-countries-using-huawei.html.

[13] Anthony Boadle and Andrea Shalal, "U.S. offers Brazil telecoms financing to buy 5G equipment from Huawei rivals," Reuters, October 20, 2020, https://www.reuters.com/article/us-usa-brazil-trade/u-s-offers-brazil-telecoms-financing-to-buy-5g-equipment-from-huawei-rivals-idUSKBN2751TA.

[14] R. Evan Ellis, "Chinese Security Engagement in Latin America," Center for Strategic & International Studies, November 19, 2020, https://www.csis.org/analysis/chinese-security-engagement-latin-america.

[15] Michael A. Matera, "The Relevance of U.S.-Caribbean Relations: Three Views," Center for Strategic & International Studies, June 2017, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170630_Matera_RelevanceUSCaribbeanRelations_Web.pdf.

[16] Cassandra Garrison, "China's military-run space station in Argentina is a 'black box,'" Reuters, January 31, 2019, https://www.reuters.com/article/us-space-argentina-china-insight/chinas-military-run-space-station-in-argentina-is-a-black-box-idUSKCN1PP0I2.

[17] "ArgenChina: Santa Cruz Será Base de un Proyecto Satelital Chino Similar al de Neuquén," OPI Santa Cruz, May 20, 2021, https://opisantacruz.com.ar/2021/05/20/argenchina-santa-cruz-sera-base-de-un-proyecto-satelital-chino-similar-al-de-neuquen/.

[18] Mat Youkee, "The Panama Canal Could Become the Center of the U.S.-China Trade War," Foreign Policy, May 7, 2019, https://foreignpolicy.com/2019/05/07/the-panama-canal-could-become-the-center-of-the-u-s-china-trade-war/.

[19] Joseph S. Nye, Jr., The Future of Power (New York: Public Affairs, 2011), 23.

[20] Ryan Dube and Luciana Magalhães, "For Covid-19 Vaccines, Latin America Turns to China and Russia," Wall Street Journal, February 24, 2021, https://www.wsj.com/articles/for-covid-19-vaccines-latin-america-turns-to-china-and-russia-11614186599.

[21] Dube and Magalhães, "For Covid-19 Vaccines, Latin America Turns to China and Russia."

[22] Ernesto Londoño and Letícia Casado, "Brazil Needs Vaccines. China Is Benefiting," New York Times, March 15, 2021, https://www.nytimes.com/2021/03/15/world/americas/brazil-vaccine-china.html.

[23] "Foreign Policy Concept of the Russian Federation," Ministry of Foreign Affairs of the Russian Federation, December 1, 2016, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248.

[24] Julia Gurganus, "Russia: Playing a Geopolitical Game in Latin America," Carnegie Endowment for International Peace, May 3, 2018, https://carnegieendowment.org/2018/05/03/russia-playing-geopolitical-game-in-latin-america-pub-76228.

[25] Sergey Sukhankin, "Will Nicaragua Become Russia's 'Cuba of the 21st Century?,'" Eurasia Daily Monitor 15, no. 118 (2018), https://jamestown.org/program/will-nicaragua-become-russias-cuba-of-the-21st-century/; and Joshua Partlow, "The Soviet Union fought the Cold War in Nicaragua. Now Putin's Russia is back," Washington Post, April 8, 2017, https://www.washingtonpost.com/world/the_americas/the-soviet-union-fought-the-cold-war-in-nicaragua-now-putins-russia-is-back/2017/04/08/b43039b0-0d8b-11e7-aa57-2ca1b05c41b8_story.html.

[26] "Convenio de 'seguridad de la información' con Rusia: una Nueva Arma del Régimen," Confidencial, August 27, 2021, https://www.confidencial.com.ni/nacion/convenio-de-seguridad-de-la-informacion-con-rusia-una-nueva-arma-del-regimen/.

[27] "Quiénes Somos," Russia Today en Español, accessed April 7, 2021, https://actualidad.rt.com/acerca/quienes_somos.

[28] Andrey Pyatakov, "Russia and Latin America in the 21st Century: A Difficult Rapprochement," Institut Françai des Relations Internationals, July 2020, https://www.ifri.org/sites/default/files/atoms/files/pyatakov_latin_america_an_2020.pdf.

[29] Polly Mosendz, "Putin Writes Off $32 Billion of Cuba's Debts to Russia," The Atlantic, July 11, 2014, https://www.theatlantic.com/business/archive/2014/07/russia-writes-off-32-billion-in-cuban-debt/374284/.

[30] Simon Shuster, "Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions," TIME, March 20, 2018, https://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/.

[31] United States House Committee on Foreign Relations Subcommittee on Western Hemisphere, Civilian Security, Migration, and International Economic Policy, "Shoring Up a Beleaguered Ally," Testimony of Ryan C. Berg, March 3, 2021, https://www.aei.org/research-products/testimony/shoring-up-a-beleaguered-ally/.

[32] "Murphy Introduces Bill to Assess China's Efforts to Expand Presence and Influence in Latin America and the Caribbean," Press Release, Office of Congresswoman Stephanie Murphy, April 13, 2021, https://murphy.house.gov/news/documentsingle.aspx?DocumentID=1689.

[33] Ryan C. Berg and Allison Schwartz, "The Dragon Descends Southwards: Chinese Foreign Policy in Latin America Warrants a U.S. Response," Georgetown Security Studies Review, May 4, 2021, https://georgetownsecuritystudiesreview.org/2021/05/04/the-dragon-descends-southwards-chinese-foreign-policy-in-latin-america-warrants-a-u-s-response/.

[34] Ryan C. Berg, "China's Hunger for Seafood is now Latin America's Problem," Foreign Policy, October 30, 2020, https://foreignpolicy.com/2020/10/30/chinas-hunger-for-seafood-is-now-latin-americas-problem/.

[35] Christopher Sabatini and Ryan C. Berg, "Autocrats Have a Playbook—Democrats Need One Too," Foreign Policy, February 10, 2021, https://foreignpolicy.com/2021/02/10/autocrats-have-a-playbook-now-democrats-need-one-too/.

[36] Alex Nowrasteh and Andrew C. Forrester, "Immigrants Recognize American Greatness: Immigrants and Their Descendants Are Patriotic and Trust America's Governing Institutions," CATO Institute, February 4, 2019, https://www.cato.org/publications/immigration-research-policy-brief/immigrants-recognize-american-greatness-immigrants.

AUTHORS

Hal Brands is a Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins University School of Advanced International Studies.

Ryan C. Berg is senior fellow in the Americas Program at the Center for Strategic and International Studies.

Margaret Myers

Beginning in February 2020, China's diplomatic community—together with Chinese provincial and municipal governments, businesses, and media outlets—set forth to shape opinions of China in the Latin American and Caribbean (LAC) region, when many in LAC had mixed views of China and its relationship with COVID-19. In the following months, China engaged not only in the delivery of personal protective equipment (PPE) and, more recently, vaccines to LAC countries but also launched an extensive messaging campaign, carried out through traditional and social media by Chinese embassies and media outlets across the region.

Analysis of trends in China's coronavirus-era engagement with LAC reveals striking developments in China's aid delivery and public messaging toward the region and also in China's broader approach to LAC relations. China's engagement with LAC amid the pandemic can be divided into two distinct phases.

- The first of these was most evident from February to around September 2020. It consisted of sales and donations of medical equipment and other forms of cooperation and assistance, such as advisory services and consultations between medical professionals from China and LAC nations, and some instances of cooperation on vaccine testing and development.[1]

- Based on a review of 470 announcements of Chinese PPE deliveries announced in Chinese, Latin American, and other media sources—as well as Chinese embassy Twitter accounts[2] —the pace of PPE deliveries slowed considerably after summer 2020 (see Figure 1), as China focused more extensively on vaccine development and distribution—the second phase in China's COVID-19 outreach.

China's COVID-19 assistance is meant to achieve wide-ranging objectives. In addition to humanitarian motivations, which are frequently underscored by Chinese officials and generally supported at home by the Chinese public,[3] China's COVID-19 aid and broader economic outreach have also sought to reinforce and strengthen bilateral ties throughout the region—to ensure, above all, that China emerges from the pandemic with its image generally intact, and to simultaneously advance some of China's commercial objectives and policy interests, including the political isolation of Taiwan.

For the companies involved in China's international outreach, the pandemic was an opportunity to highlight their commitment to those countries and communities where they operate. For China's tech firms, the pandemic also provided an opportunity to showcase new biomedical technologies and artificial intelligence-enabled diagnostic capabilities.

In the early months of the pandemic, China employed a notably decentralized aid campaign, leveraging wide-ranging Chinese actors and on-the-ground networks to deliver medical supplies to LAC nations.

It entailed loosely coordinated engagement by wide-ranging Chinese actors, including Chinese embassies, companies, provincial government authorities, networks of overseas Chinese communities, and quasi-governmental organizations, such as the Chinese Red Cross. This approach was targeted and flexible, allowing for often-impromptu donations to hard-hit communities, local organizations, and individuals capable of influencing China's broader commercial and political interests.

China's initial "aid blitz," whether delivered by Chinese companies, embassies, overseas communities, the Chinese Red Cross, or other actors, was carried out at a pivotal moment for global opinion on China and COVID-19.

Amid mounting critiques and accusations, China sought to position itself in LAC and other regions as a responsible actor and proponent of cooperation at a moment of global crisis.[4] Much of this work fell to China's embassies, which, in addition to coordinating donations and sales of PPE and vaccines, labored throughout the pandemic to convey specific messages about China's experience with the coronavirus and its pandemic outreach.

Of interest in China's communications campaign was an increase in assertive messaging in the early months of the pandemic, characteristic of the so-called "wolf warrior" diplomacy that featured prominently in academic and policy accounts of China's external communications in spring 2020. In most cases, China's sharp-edged defensive rhetoric was accompanied by promotional messaging, which, along with an emphasis on cooperation and multilateralism, has since dominated China's communications with the region.

Recent efforts to isolate Taiwan mark a clearer-than-ever departure in LAC from China's long-standing policy of noninterference. China has been effective, in the short term at least, in using its role as a provider of vaccines to the region to quell criticism of China and influence Taiwan-related policymaking.

China, directly and indirectly, encouraged Taiwan's allies to rethink their diplomatic allegiances. Beijing

suggested that Honduras seek a "diplomatic bridge" to purchase Chinese vaccines, for instance.[5] China also sought to influence Taiwan's relations with Paraguay by conditioning the transfer of vaccines on changes in those countries' Taiwan policies. Guyana received 200,000 doses of Chinese vaccine after deciding to close a new commercial office with Taiwan.

Vaccines have also been used to reward or discourage other LAC government actions. In Brazil, China reportedly halted the shipment of raw materials necessary for the São Paulo-based Butantan Institute to produce China's CoronaVac vaccine[6] after President Jair Bolsonaro suggested that China disseminated COVID-19 as a tactic of biological warfare.[7]

Despite the efforts of wide-ranging Chinese actors, China's COVID-19 diplomacy has been more successful in advancing some of China's objectives than others.

- China's extensive messaging campaigns and medical assistance arguably helped avoid an image crisis at the pandemic's onset.
- China's decentralized approach provided it with considerable flexibility and visibility when operating in LAC. By deploying on-the-ground assets to support China's diplomatic objectives, China was able to respond in near real-time to developments in the region, changing course as needed.
- China's LAC-based entities were also able to target the delivery of numerous, small donations to specific communities and individuals, in occasional support of broader commercial and political interests.
- China's approach was also occasionally problematic, however. Francisco Urdinez has noted the challenges of coordinating China's decentralized approach, including occasional miscommunications and diplomatic blunders.[8] In Chile, poor coordination among Chinese actors resulted in a serious misunderstanding with Chilean officials.[9] Courting LAC officials with PPE kits and vaccines is also a problematic and potentially corruption-inducing practice.
- China's experiment with "wolf warrior"-type messaging may have had unintended effects, as Yale University's Daniel C. Mattingly and James Sundquist noted. Wolf warrior diplomacy, they say, has backfired on numerous occasions.[10]
- Our analysis of tweets from the LAC region suggests that while LAC audiences possibly view China as more impactful on LAC affairs than before the pandemic, they are still ambivalent about China and its influence in the region. We noted a substantial overall increase in LAC tweets about China during the pandemic. Before the pandemic, 41,098 geo-referenced tweets mentioned China. More than three times as many (144,181 tweets) referenced China during the pandemic. The terms used in these tweets were not strongly positively or negatively weighted, however.[11]
- The effects of China's outreach may be more striking in the commercial realm in LAC, to the extent that Chinese companies have indeed solidified or generated new ties amid the pandemic. Any benefits to Chinese companies from their extended outreach could take considerable time to materialize, however, and will undoubtedly vary on a company-by-company basis. LAC Twitter users referenced Huawei fewer times during the pandemic (5,376 tweets) than before (7,870 tweets), despite the company's relatively robust pandemic outreach.
- As Financial Times Latin America Editor Michael Stott noted in a May 2021 Inter-American Dialogue event, it is probable that neither China nor U.S.-China competition are foremost for most in LAC at this juncture. LAC leaders, in most cases, are seeking critical COVID-19 solutions, regardless of their source.

Ultimately, this exercise has been an experimental one for China, whether through the use of an impromptu and often-decentralized aid campaign, the development of new medical technologies, or by employing novel approaches to communications with the region. China's approach has supported numerous objectives, whether economic or diplomatic, but wide-ranging factors will determine the overall impact of Chinese outreach. These include the effectiveness of Chinese vaccines and the extent of commitments by partner nations during the pandemic and after, as LAC prepares for a period of prolonged economic and social recovery.

REFERENCES

[1] Wanming Yang, Twitter post, April 9, 2020, twitter.com/WanmingYang/status/1248435532306075654.

[2] Chinese embassies in Argentina, the Bahamas, Brazil, Chile, Colombia, Cuba, Dominican Republic, Ecuador, El Salvador, Grenada, Peru, and Venezuela have active Twitter accounts.

[3] Observation is based on author review of reader commentary in Chinese-language Weibo posts about China's vaccine diplomacy. The vast majority of comments

by Chinese netizens reflected a positive view of China's overseas outreach. Numerous posts included the phrase, "大国担当"" ("acting like a great power").

[4] Steven Lee Myers and Alissa J. Rubin, "Its Coronavirus Cases Dwindling, China Turns Focus Outward," *The New York Times*, March 18, 2020, www.nytimes.com/2020/03/18/world/asia/coronavirus-china-aid.html.

[5] "China is seeking to use Covid-19 vaccines for political gain with Honduras move, says Taiwan," *The Straits Times*, May 12, 2021, www.straitstimes.com/asia/east-asia/taiwan-says-china-seeking-political-gain-with-honduras-vaccine-move.

[6] "Brazil needs to resolve diplomat issues with China for COVID-19 vaccine: Sao Paulo governor." *Xinhua*, June 6, 2021, www.xinhuanet.com/english/2021-05/15/c_139947542.htm.

[7] "Bolsonaro suggests coronavirus is part of China's biological war," *Brazilian Report*, May 5, 2021, brazilian.report/liveblog/2021/05/05/bolsonaro-suggests-coronavirus-is-part-of-chinas-biological-war/.

[8] Francisco Urdinez, "China's Improvised Mask Diplomacy in Chile," Carnegie Endowment for International Peace, April 6, 2021, carnegieendowment.org/2021/04/06/china-s-improvised-mask-diplomacy-in-chile-pub-84251.

[9] Urdinez, "China's Improvised Mask Diplomacy in Chile."

[10] Daniel C. Mattingly and James Sundquist, "Public Diplomacy and Its Limits," Yale University, January 26, 2021.

[11] We compared monograms from mined tweets with the AFINN lexicon dictionary published by the Technical University of Denmark and the NRC Word-Association Lexicon published by Mohammad and Turney. We then assigned an emotional weight to the top 200 words featured in tweets about China, both pre- and during the COVID-19 pandemic.

AUTHOR

Margaret Myers is the director of the Asia & Latin America Program at the Inter-American Dialogue.

Vladimir Rouvinski

"[Russia needs] a channel that people are used to; one they like and [that can be ready to expose its audience to the required information feed]. In a sense, not having your own foreign broadcasting is like not having a ministry of defense. When there is no war, it seems like [media in foreign languages] is not needed. But [...] when there is war, this is directly critical. But you can't create an army a week before the war has begun."

Margarita Simonyan (RT editor-in-chief), "Russian media from inside," Afisha Daily, October 18, 2011

Russia's return to the Western Hemisphere

During the Cold War, Latin America and the Caribbean served as a stage for power competition between the United States and the Soviet Union. The logic of a bipolar world guided the policy design of Washington and Moscow. After the 1991 collapse of the Soviet Union, new Russia lost its interest in the region. Facing enormous economic difficulties, the government of Boris Yeltsin collaborated with the United States on various international agenda topics. Yet, at the beginning of the new century, under the government of Vladimir Putin, Russia returned to the Western Hemisphere. While there are several reasons behind Russia's return, the notion of reciprocity is the foremost factor.

The majority of the elites that govern Russia today view the entire Western Hemisphere as Washington's priority area of political, economic, and social concern. Similarly, the top officials of Putin's government consider the territory of the former Soviet Union, a "near abroad," as the most important geographical area outside Russia's borders. Russian leadership is convinced that Moscow has the right to have special interests in this "near abroad" because of historical, cultural, and economic ties. Hence, post-Soviet Russian leaders insist that all governments outside the region must consider Russia's special interests before advancing their relations with the countries of the former Soviet Union.

Symbolic reciprocity has multiple manifestations in the realm of Russian foreign policy. First, it is an opportunity for Putin's government to show that Russia can respond reciprocally to what is perceived by the Russian elites as destructive actions by the U.S. government in Moscow's "near abroad." For example, during the crisis in Georgia in 2008, the Russian government expressed its concerns regarding the U.S. naval presence in the Black Sea and the support Washington offered to anti-Russian forces.[1] Moscow sent its strategic bombers and naval ships to the Western Hemisphere right after the five-day war between Russia and Georgia in 2008. Moreover, the signs of increased military cooperation with Nicaragua, Venezuela, and Cuba coincided with the annexation of Crimea in 2014 and U.S. support of Kyiv.[2] The active participation of Moscow in Venezuela's latest crisis is yet another manifestation of the symbolic reciprocity approach in Latin America. At the same time—and since Russia has limited conventional resources—it resorts more frequently to asymmetrical methods than traditional engagement to pursue a policy of reciprocity. Strategic communication is one of the tools of that policy.

The modus operandi of Russia's strategic communication

In today's globalized world, states use strategic communication to enhance their capabilities abroad and facilitate foreign policy objectives via long-established activities, including public diplomacy, public affairs, nation branding, and information operations. After Putin came to power, Moscow opted not simply to broaden the scope of its communication overseas but to exercise "sharp power" through solid mechanisms that could effectively disseminate desired values, interests, and goals. Coined by Christopher Walker and Jessica Ludwig,[3] sharp power describes efforts that seek to pierce, penetrate, and perforate the political and information environments of targeted countries. In this context, Russian strategic communication in Latin America is Moscow's principal vehicle of sharp power. It enables the Putin government to cut into the fabric of Latin American society, amplifying existing political divisions, questioning liberal democratic order, and diminishing U.S. influence in the region.

Although contemporary global communication may use various channels to reach targeted audiences, Russia's modus operandi in Latin America relies heavily on government-controlled mass media, namely, RT television networks and the Sputnik news agency in Spanish. As part of Putin's foreign strategy, Russian foreign-language broadcasting targets viewers in Latin America because Moscow presumes it is easier to attract new audiences there than compete with established media outlets in the United States and Western Europe. As globalization and economic liberalization increased cultural exchanges in the southern part of the Western Hemisphere in the 1990s and 2000s, Latin Americans requested broader coverage of political and international topics than the mainstream local media offered. Nevertheless, the offer remained limited.[4] Hence, from the Russian perspective, media markets would respond favorably to new international broadcasters in Spanish if the new outlets would provide a different perspective on critical subjects of public interest. Although RT started in 2005 by broadcasting in English to viewers

in English-speaking Western countries, it later turned a considerable share of its attention to Latin America. The success of Russian efforts to reach a wider audience is evident by the number of RT's followers on the internet, affiliated TV cable providers, and geographical scope.

In 2021, only 12 years after its first Spanish-language broadcast, RT is readily available everywhere in the region. In some cases, the channel is made available as part of public TV broadcasting systems (Argentina, Venezuela, and Cuba) or as part of the state satellite system (Bolivia). In other countries, such as Colombia, hundreds of small local cable networks retransmit RT programming in addition to Claro, the principal cable provider in the country. Moreover, RT pays cable operators to carry its signal on allied networks, making it difficult to end collaboration with Moscow; in many cases, Russian funding helps smaller operators survive in the market. RT also has agreements to broadcast programs on local channels; viewers are often unaware the information they receive comes from Russia. This approach allows RT to extend the reach of Russia's strategic communication to potentially millions of additional viewers in Latin America. Besides, RT is freely available 24 hours per day and online. As a result, in September 2021, RT in Spanish on Facebook[5] had more than 18 million followers. The RT YouTube channel in Spanish had over five million subscribers,[6] and RT Play in Spanish on Facebook had more than six million.[7] Finally, more than 3.5 million people follow RT in Spanish's Twitter account.

However, the analysis of the presence of Russia's government-sponsored media would be incomplete without mentioning the Sputnik news agency. This media outlet maintains its own websites in addition to traditional and digital radio broadcasting in three-dozen languages, but it is part of the same organizational framework as RT. Sputnik's Spanish-language branch is Sputnik Mundo.[8]

Despite the diversity of programs and media platforms, a close examination of the content produced by RT in Spanish and Sputnik Mundo reveals several standard features. First, there is the inclusion of politically unrelated news and reports like sensationalized bulletins in its feeds. This strategy aims to recruit new followers who otherwise might not be interested in getting information from RT or Sputnik. It also provides Russia with the potential to use a CNN-like effect understood as real-time communication to provoke the desired response from foreign audiences. Second, the main political narratives employed by Russian media for foreign audiences support the official position of the Russian government. It is not to say that RT and Sputnik focus exclusively on Russia's foreign policy agenda. Yet, it is a clear priority of its information coverage. Third, RT's global "information menu" is designed to take advantage of opportunities unique to each region. In Latin America, many of RT's politically sensitive programs align with narratives promoted by political forces to the left of the political spectrum. However, some other programs, which have millions of views, often are anchored by celebrities associated with political forces other than the Latin American left. For instance, during the 2018 World Cup in Russia, RT hired Carlos Valderrama, one of South America's most recognizable soccer players. Regarding Colombian politics, Valderrama supported the right-centrist U party of then-Colombian President Juan Manuel Santos. With Latin American societies becoming ideologically more polarized, RT's potential looks promising for Moscow. By using its media outlets, Russia can reach out to various segments of the population and skillfully apply sharp power by questioning established facts related to sensitive topics for some viewers. This approach is particularly noticeable when it comes to the coverage of U.S.-related developments.

RT in Spanish and Sputnik Mundo's narratives

While the narratives delivered through RT and other news agencies emphasized the role of Russia as a global player, they also stressed that the United States resisted the process of Russia regaining its influence in the international arena and opposed building a new multipolar order with Latin American partners. Moscow is seeking to misinform viewers regarding U.S. policy on other topics, including migration, liberal democracy, and economic and social issues. In recent years, two items have been foremost on that agenda: the crisis in Venezuela and the COVID-19 pandemic.

The most important Venezuela-related narrative fits perfectly with the logic of symbolic reciprocity: "The United States wants regime change." Russian media interprets the opposition struggle as Washington's attempt to change the unfriendly regime in Caracas, identical to the "color revolutions" in Russia's "near abroad." According to Russian government-controlled media, these efforts bring about the deterioration of living standards, the suffering of ordinary people, and widespread violence. Furthermore, as part of Russia's strategic communication agenda, RT is mobilized to provide information backing Nicolás Maduro's regime while justifying Moscow's aid to Caracas as a necessary move to protect the world "against malign U.S. intentions." RT aimed to discredit Juan Guaidó and cast doubts on his legitimacy and capacity to govern. Since the beginning of the latest crisis in Venezuela in January 2019, the channel has aired more than 300 reports with Guaidó's name in the headlines of its newsfeed. Another story line is dedicated to the impact of U.S. sanctions. RT tried to convince its viewers that the main reason behind Venezuela's catastrophic situation was not the disastrous economic

policy of the Chavista government but, rather, U.S. sanctions. In this context, RT dedicated numerous reports to praising the efforts of Maduro's government to govern the country with timely assistance offered by Moscow.

The COVID-19-related strategic communication originating in Russia and destined for Latin America took full advantage of the introduction of the "Sputnik-V" vaccine and the beginning of the "COVID vaccine race." First, the news of the Sputnik-V vaccine was interpreted as evidence of Russia being one of the most technologically advanced nations, which is often denied because of bad publicity originated in the Western media. In addition, RT and Sputnik Mundo alleged that pro-U.S. Latin American governments were unwilling to acquire the Russian vaccine—not because it does not comply with the necessary protocols and tests, but because of their political ties with Washington. This type of strategy has created several noticeable tensions in the Latin American information space. In December 2020, for example, RT's Inna Afinogenova skillfully engaged the popular Colombian newsmaker Vicky Davila in a public debate about the role of Russian media in Latin America when reporting on sensitive topics like COVID-19. The debate attracted the attention of many viewers who otherwise would be unaware of RT in Spanish. In 2021, Russia signed agreements to start producing the Sputnik vaccine in Argentina and negotiating the delivery of Russian vaccines to other Latin American countries. Therefore, there is little doubt that Moscow will continue to exploit politically sensitive topics such as the COVID-19 vaccine.

Beyond disseminating Moscow's overarching narratives in Latin America

By 2021, RT and other Russian government-sponsored media had become a familiar source of information in the Spanish-speaking world of the Americas. The Kremlin managed to restore the possibility of being exposed to an alternative view to the one promoted by the United States and democratic governments in the region for the first time since the dissolution of the Soviet propaganda machine. Contemporary Russian information coverage is once again an aggressive, purposeful intervention in the international media space that goes beyond the dissemination of Moscow's overarching narratives.

One of the factors behind RT's success in Latin America is the public's lack of understanding of the nature of Moscow's interest in the region's information space. Many Latin Americans perceive the growing incidence of Russian media as something "normal," part of the exercise of freedom of expression and diversity of opinions. However, it is part of a foreign policy strategy designed to achieve specific objectives by the Putin government. Russia thrives on communicating desired explanations for important developments with comfortable ease and makes it difficult for democratic governments to repair the damage. The sharing of democratic values among the countries of the Western Hemisphere is the key to security in the region; the prevalence of like-minded democracies makes the political geography of the Western Hemisphere unique. Since Russia is not a democracy, RT and Sputnik Mundo often refer to democracy as a political regime with many weaknesses. In this context, one of the long-term goals of Russia in Latin America is to carry out continuous strategic communication via government-controlled outlets to undermine the idea of democratic order.

The advance of Russia's strategic communication in Latin America has almost no opposition. There have been only a few public debates on RT and Sputnik in the regional information space. Therefore, it is necessary to continue raising the awareness of decision-makers and the Latin American public regarding the nature of Russia's government-controlled mass media. At the same time, it is vital to challenge Russia's strategic communication by escalating government-led efforts. While the United States promotes its political culture by supporting democratic movements and local mass media in Latin America, U.S. media consists of predominantly commercial outlets. The mainstream media in English is the first choice of highly educated Latin Americans, a minority in the region. CNN en Español (2.5 million subscribers on YouTube, many based in the United States), CNN Chile (0.5 million subscribers), CNN Radio Argentina, and several others have established impressive audiences. Still, their further growth depends on market factors. Currently, U.S. government-sponsored information outlets have limited reach in the region. For instance, as of September 2021, Voice of America in Spanish has only 180,000 subscribers on YouTube compared to the millions of followers of RT and Sputnik. From this perspective, Russia's strategic communications have a broader reach to those segments of Latin American societies that—in the context of growing economic and social difficulties in the region—might be willing to endorse views originating in Moscow.

Despite some similarities, overall, it is difficult to consider the current confrontation of Putin with the West as a new cold war. Post-Soviet Russia neither military nor economically matches the USSR, and the Kremlin's objectives are different from those promoted by Soviet leadership. Nevertheless, many Russian decision-makers consider that Russia is at war—not a "hot war," but a new kind of confrontation characterized by a comparable level of symbolic tension with the United States and its allies as during the Cold War. Moreover, elites

in Moscow are convinced there is little hope the pressure will ease anytime soon. In this context, Russia will attempt to sustain and expand its strategic communication in Latin America via RT in Spanish, Sputnik Mundo, and other media outlets as a cost-effective tool of its foreign policy.

REFERENCES

[1] In 2008, some of the titles of the news reports by Russia's government-controlled media were: "Russia is concerned about the buildup of NATO ships in the Black Sea," Ria Novosti, August 25, 2008, ria.ru/20080825/150651454.html; "Putin: Russia will respond to the presence of foreign ships in the Black Sea," Ria Novosti, September 2, 2008, ria.ru/20080902/150896338.html; and "Russian Foreign Ministry doubts Mount Whitney's humanitarian mission in the Black Sea," Ria Novosti, September 5, 2018, ria.ru/20080905/150997668.html.

[2] In 2014, Russia's reaction was similar to that of 2008. See, for example, "US Navy destroyer Donald Cook entered the Black Sea," Tass, April 10, 2014, tass.ru/mezhdunarodnaya-panorama/1112077. Soon after Cook's mission to the Black Sea was over, Russia supplied anti-aircraft artillery to Nicaragua valued at US$15 million. Before 2014, Moscow's support to Managua consisted of non-lethal supply only. See Roberto Canjina, "Armed to the Teeth: Nicaragua's Remilitarization," Envio Digial, October 2016, www.envio.org.ni/articulo/5266. In July 2014, the Russian and Cuban governments had discussed reopening the Soviet-era Lourdes signal intelligence post designed to spy on the United States. See "Imeyushchiy ushi da vnov' uslyshit: Rossiya vozvrashchayet na Kubu svoy tsentr radioperekhvata," Kommersant, July 16, 2014. Also, in July 2014, Putin agreed to open a new credit line to Venezuela for buying new Russian weapons, among other things. See "Rusia aprueba linea de crédito a Venezuela," BBC.com, July 17, 2014, www.bbc.com/mundo/ultimas_noticias/2014/07/140717_ultnot_venezuela_rusia_credito_jgc.

[3] Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence," Foreign Affairs, November 16, 2017, www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.

[4] Toril Aalberg and Stylianos Papathanassopoulos et al., "International TV News, Foreign Affairs Interest and Public Knowledge," Journalism Studies, 14 (3) (2013): 387-406. Similar conclusions can be made after examining the results of the project The Americas and the World, published online at www.lasamericasyelmundo.cide.edu/, accessed September 14, 2021.

[5] RT en Español Facebook webpage, www.facebook.com/ActualidadRT/.

[6] RT en Español YouTube channel, www.youtube.com/channel/UC2mtXUpAYLYJIZ2deSPhlqw.

[7] RT Play en Español Facebook webpage, www.facebook.com/esRTmedia/.

[8] Sputnik Mundo webpage, mundo.sputniknews.com/.

[9] For example, the most popular videos published by RT on YouTube are not politically related. See the list of the videos available at RT en Español's YouTube webpage: www.youtube.com/c/RTenEspa%C3%B1ol/videos?view=0&sort=p&flow=grid, accessed September 14, 2021. See also Gordon Ramsay and Sam Robertshaw, "Weaponising News RT, Sputnik and Targeted Disinformation," King's College London Centre for the Study of Media, Communication & Power, 2019, www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf, accessed September 14, 2021.

[10] "El Pibe, a la cancha política por La U," El Heraldo, November 29, 2013.

[11] See, for example, "Cinco años de sanciones de EE.UU. contra Venezuela: ¿Un crimen a fuego lento?," RT Actualidad, March 8, 2020, actualidad.rt.com/actualidad/343356-cinco-anos-sanciones-eeuu-venezuela-crimen.

[12] Voice of America YouTube channel, www.youtube.com/channel/UCJ46VgZgCMLFUvOT671AOJw.

AUTHOR

Vladimir Rouvinski is director of the Laboratory of Politics and International Relations and associate professor, Department of Political Studies, Icesi University, Cali, Colombia.

Betilde Muñoz-Pogossian & Diego Chaves-González

Migrants from Central America have moved in large numbers in recent years. According to the most recent Global Trends Report of the United Nations High Commissioner for Refugees (UNHCR), the total number of asylum seekers, refugees, internally displaced persons, and returnees from Central America was 107,407 in 2014, while a total of 905,796 were registered by 2019. The arrival of so many internally displaced populations (IDPs), migrants, and refugees has created challenges and opportunities for countries in the region. Natural disasters and the COVID-19 pandemic have only added complexity to the situation.

As it has become clear that many displaced migrants will remain abroad for an extended period, if not permanently, the focus has begun to shift from the provision of humanitarian aid to understanding the root causes of migration to strengthen the countries of origin preparedness, infrastructure, access to services, and institutional reforms to address the situation. These measures hold the potential to benefit the displaced populations, migrants and refugees, and the communities in which they live by boosting economic development and social equity and reinforcing social cohesion.

To examine the link between climate change and human mobility of migrants and refugees in this region, this article analyzes data from the Internal Displacement Monitoring Centre (IDMC), Armed Conflict Location & Event Data Project (ACLED), United Nations Office on Drugs and Crime (UNODC) studies, and various data from other sources, reports, and additional research resources. The report explores the correlation between three key dimensions that could trigger factors for human mobility northward—natural disasters, internal displacement, and violence—across the three Northern Triangle countries (El Salvador, Guatemala, and Honduras). Together they comprise 86 percent of Central Americans arriving at U.S. borders, and as of 2017, eight percent of the United States' 44.5 million immigrants.[1]

This study also examines the correlation of these variables across time, considering the accumulation (sum) of episodes in three years of variable *b,* which has a correlating effect on variable *a*. For example, when correlating natural disasters in any given year with the number of internally displaced population, this investigation totaled the number of internal displacements in the three consecutive year period and then correlated this number with the natural disasters that happened at any given year.
Consequently, this research looked at answering the following questions: is there a connection between the increase in the frequency and severity of climate events in Central America and migration? How would this relationship come about? What role does internal migration play? And what impact does the forced internal displacement of these populations affected by climate events have on community social and security conditions? Can internal displacement explain violence in these countries? And how do these impact these populations' move toward the North?

The article answered these questions by answering whether *internal displacement caused by natural events is an underlying factor that incubates violence and social instability, and if forced migration northward stimulated by violence should also be associated with the frequency of natural events*.

The analysis suggests all variables correlate positively. However, correlations are stronger when analyzing internal displacement and violence and violence with out-migration. The data and analysis of the findings presented in this report provide a valuable indication of trends and insights to support effective policymaking in the region.

These were then crossed following the transitivity principle.[2] In this case, the hypothesis is that if natural disasters correlate with internal displacement in the Northern Triangle countries, they could increase the number of homicides (used as a proxy for violence) in the region. The increase in violence could be correlated with migration toward northern countries (Mexico, the United States, and Canada). Two important caveats to keep in mind is that correlation does not imply causation. Although there might be a correlation between the variables, one cannot make any claims of causality between the different variables solely based on the existence of this correlation. Secondly, we discovered a limitation of available data in this case, which could provide an important opportunity to identify new gaps in the prior literature and present the need for further development in this area of study. These two caveats are explored further in the following sections.

Results

The results corroborate previous studies relating to the relationship between migration, internal displacement, conflict, and natural disasters. After running the four different correlations that this report proposes, the findings suggest a weak but positive correlation between natural disasters and internal displacement. In other words, the findings indicate that the existence of floods, hurricanes, or earthquakes, among other natural events, may not be the only determinant of internal displacement in these

three countries. Still, it is definitively influencing people's decision to move. As more variables are included in the correlations and more factors are considered, the correlations get more potent, as Figure 1 shows.

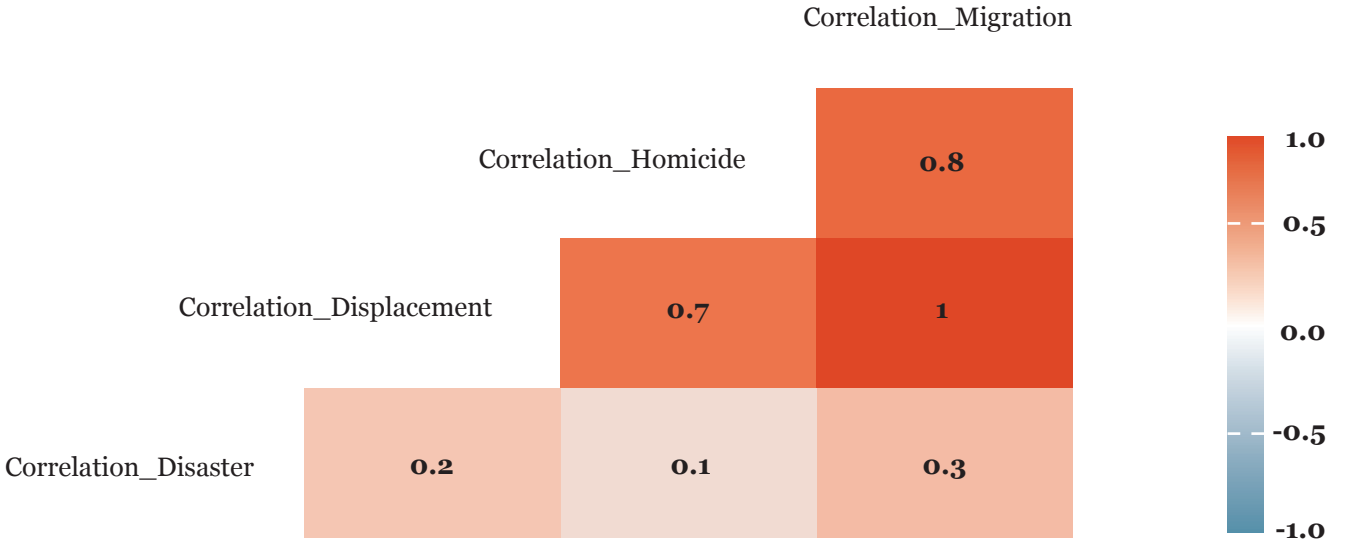
When assessing the second correlation between internal displacement due to natural disasters and homicide, the correlation coefficient is 0.7. This shows that the relationship between internal displacement caused by natural disasters and homicide is strong. This correlation coefficient was found by comparing the three-year sum of the internally displaced people due to natural disasters in each country with the total homicides in the region. In other words, there is evidence that internal displacement caused by natural disasters in these three countries may exacerbate violence measured by the number of homicides occurring in communities that have received IDPs due to natural disasters. Since this correlation between IDPs due to natural events and homicides is strong, this study recommends further studies that account for other factors and use alternative methodologies such as linear regressions.

Moreover, there is a correlation between homicide and migration. The correlation coefficient, in this case, is 0.8. When testing for the significance of this coefficient, the p-value was 0.031. Given these results, there is an essential and strong correlation between homicide and migration toward the North. What Figure 1 suggests, then, is that this study shows strong results when it comes to the correlation between homicide and migration toward the northern countries. As it still exists to some degree, a correlation between displacement and natural disasters (r=0.220), did not yield a significant result at the 90 percent confidence level. Therefore, this study cannot rule out the possibility there might not be a correlation at all. In other words, all variables are positively correlated. However, as we crossed the different variables, the levels of correlation became stronger.

Furthermore, the significance tests applied, and which measure the confidence levels, rejected the null hypothesis of this research. In this sense, this study is an invitation to create more accessible data on human mobility associated with environmental factors that are sufficient and of quality. Thus, the region could make visible and provide a better understanding and attention to migration triggers, allowing and thereby substantiating policies, actions, and decisions at the regional and national level.

Putting these results into perspective and contextualizing them, as Figure 2 shows, the correlations intensify as more variables are factored into the model. This report argues that this is the case since emigration is a process that occurs progressively after an initial shock (in this case, natural disasters). The study accounts for countries that have suffered years of deterioration and have not improved their resilience mechanisms to defend themselves against these shocks. Thus, there are increases in internally displaced populations and migrants who look for opportunities in Northern countries.

Figure 2: Intensity of correlation between natural disasters and migration toward the North



Source: Prepared by the authors

After assessing the results, the report suggests different reasons explaining the results. First, looking at the results from a vulnerability perspective, when a natural disaster strikes a country, the level of vulnerability that individuals face has a certain impact. However, as displacement begins to occur because of these disasters, their vulnerability levels increase, reflecting why correlations get stronger.

Figure 3. Country of Hazard Type.

Hazard Type	El Salvador	Country Guatemala	Honduras
Drought			1
Dry mass movement		2	1
Earthquake	3	6	2
Extreme Temperature		6	
Flood	11	25	20
Storm	5	5	4
Volcanic Eruption	1	6	
Wet mass movement	2	3	
Wildfire			1

Source: Prepared by the authors

Data related to violence, conflict, and economic factors prevail as primary triggers of human mobility in the region. Other more easily identifiable factors often hide the environmental trigger, either by the absence of studies and the production of specific data, practical and methodological difficulties to generate this type of data, or the limited perception of the environmental factor as a mobility inducer. It is necessary to reinforce the relationship between multiple vectors of mobility in the region and, especially, how environmental factors are the trigger and are related to economic vulnerability, insecurity, conflict, and violence.

Generating evidence and data about the phenomenon requires two aspects: (i) developing, testing, and validating specific methodologies, and (ii) reinforcing, improving, and coordinating methodologies and existing data sources. The absence of characterization and precise definition of the phenomenon and its categories and a defined and coherent methodology with the region's specificities are the main barriers.

It is necessary to invest in data production systems with integrated indicators on the environment and human mobility. This can generate a set of regional indicators of human mobility induced by climate change and disasters, which requires an integrated analysis and coordination between different databases and data sources and the development of specific methodologies.

This study, therefore, indicates the need to expand the availability of specific data, identify and fill gaps in data on the phenomenon, produce new data where it does not exist, and develop methodologies, standards, and common protocols for harvesting, analysis, and data collection. In addition, creating collaborative platforms for the dissemination and exchange of data to improve its accessibility and applicability is highly recommended.

REFERENCES

[1] Allison O'Connor, Jeanne Batalova, and Jessica Bolter, *Central American Immigrants in the United States,* Migration Policy Institute, August 15, 2019, www.migrationpolicy.org/article/central-american-immigrants-United-States-2017.

[2]Transitivity principle in which, if A influences B, and B influences C, then C must also be influenced by A.

[3]When we tested for the significance of the Pearson correlation coefficient, the p-value obtained is 0.063, which is lower than the alpha level of 0.10 (confidence interval of 90 percent), so we can reject the null hypothesis.

[i]United Nations High Commissioner for Refugees, 2020 Global Trends Report (Geneva: UNHCR, 2021).
Arango, Joaquín. September 2000. "Enfoques conceptuales y teóricos para explicar la migración." Revista Internacional de Ciencias Sociales, No 165: 33-47.
Bermeo, Sarah, and David Leblang. April 2, 2021. "Climate, Violence, and Honduran Migration to the United States." Brookings.
Cornelius, Wayne A. 2004. "Controlling Migration: A Global Perspective." Stanford University Press.
Fernández de la Reguera Ahedo, Alethia, Lucia Gandini, Eduardo Gutiérrez, and Juan Carlos Narvaez. 2018. "Caravanas migrantes: las respuestas de México." Serie Opiniones Técnicas sobre Temas de Relevancia Nacional, National Autonomous University of Mexico.
Gandini, Luciana and Mauricio Padrón Innamorato (Coords.) 2014. "Población y trabajo en América Latina: abordajes teórico-metodológicos y tendencias empíricas recientes." Serie Investigaciones N.º 14, ALAP Editor, México, Fondo de Población de la Naciones Unidas (UNFPA)-UNAM-Instituto de Investigaciones Jurídicas-Centro Regional de Investigaciones Multidisciplinarias-Programa Universitario de Estudios del Desarrollo.
Gómez Walteros, Jaime Alberto. January-June 2010. "La migración internacional: teorías y enfoques, una mirada actual." Semestre Económico, vol. 13, núm. 26: 81-99.
Haas, Hein de. 2008. Migration and Development, A theoretical Perspective. Working Paper. International Migration Institute, University of Oxford, paper 9.
Hollified, James F., Philip L. Martin, and Pia Orrenius. 2014. Controlling Immigration: A Global Perspective. Stanford University Press.
Inter-American Development Bank et al. 2017. "Food Security, and Emigration. Why people flee, and the impact on family members left behind in El Salvador, Guatemala, and Honduras."
Massey Douglas S., Joaquin Arango, Graeme Hugo, Ali Kouaouci, Adela Pellegrino, and J. Edward Taylor. 1993. Theories of international migration: A review and appraisal. Population and Development Review 19, no. 3: 431-66.
Roth, Benjamin, Amanda Huffman, and Robert Brame. 2020. "Too Afraid to Stay: Measuring the Relationship between Criminal Victimization in Central America and the Intent to Migrate." Crime & Delinquency.
Sánchez-Toledo, Anabel Cruz. November 2009. Migración y desarrollo. El caso de América Latina. Contribuciones a las Ciencias Sociales.

AUTHORS

Betilde Muñoz-Pogossian is director of the Department of Social Inclusion of the Secretariat for Access to Rights and Equity at the Organization of American States.

Diego Chaves-González is a migration expert at the World Bank Group and Senior Manager for the Latin American Initiative at the Migration Policy Institute.

Louise Marie Hurel

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

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

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

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

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

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

Who's great? Great Power blindfold?

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

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

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

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

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

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

From regional developments to countries views on international cyber norms

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

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

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

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

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

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

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

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

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

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

(Source: GGE[26]/OEWG)

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

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

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

AUTHOR

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

Marcus Allen Boyd & Samuel Henkin

Transnational organized crime (TOC) is a significant and growing threat to the security of the United States and a major security challenge in other critical regions of the world. TOC continues to expand dramatically in size, scope, and influence with major destabilizing effects. In recent years, TOC entities have embraced new, and often violent, practices and advanced strategies to circumvent the traditional norms of legal economies and evade security interventions often operating through a vast economic system of dark networks and economies—illicit and illegal sourcing, labor inputs, production, products and services, supply chains, and consumer operations.[1] Within these clandestine systems, TOC entities are expanding their operations, diversifying their activities, as well as exploiting the increased blurring between illicit and licit activities. The rapid evolution of TOC entities in the past 15 years has engendered a more convoluted, violent, and destabilizing convergence of threat vectors challenging security regimes in detecting, disrupting, and dismantling the (il)licit and (il)legal of transnational criminal enterprises.

The Shadow Economy of Transnational Organized Crime

The typical consumer only ever experiences the point of sale for the illicit/illegal good. They do not see the hierarchical structures and transnational trade that undergirds their purchase. The shadow economy, as Medina and Schneider notes, goes by many names and, depending on how it is defined, represents a significant share of global GDP. For example, among 158 states the average size of a state's shadow economy relative to their GDP was 31.9% between 1991 and 2015[2]. By some estimates revenues generated by transnational crime are estimated to be worth as much as $2.2 trillion annually[3]. This, of course, does not account for the countless other goods and services illicitly and/or illegally produced and purchased around the world not captured in estimates.

In this piece, we will demonstrate the general hierarchical structure of TOC entities that promulgate a significant proportion of the shadow economy and, in turn, how the existing legitimate economic structures make TOC entity activities profitable and difficult to curtail. At their core, TOCs are driven by market forces and opportunity, and they seek to maximize and sustain profits, similar to licit businesses. Yet while TOC entities operate like other legitimate businesses, albeit with (il)legal/(il)licit goods and services, they actively work to circumvent, evade, and ignore economic norms exercising corrupt, exploitative, and violent means to perpetuate their profit maximization.

The shadow economy consists of two different economies: The illicit economy and the illegal economy. The illicit economy is akin to the informal economy, that is, activities that are largely legal—selling food and other goods. These activities become illicit when they are done "extra-institutionally;" meaning the proceeds are not taxed and are not "recorded" by the government, or the proper permits and other bureaucratic operating requirements are not met. None of these activities are captured in national GDP estimates.[4] Conversely, the illegal economy consists of productive activities that run counter to domestic and/or international law. Some illegal productive activities (e.g., production of narcotics and drugs) are profitable enough to indirectly impact GDP, while others typically do not.

TOC entities thrive in the shadow economy because they are institutionally adept at navigating between the (il)licit and the (il)legal. In a recent radio interview, sociologist Federico Varese who primarily focuses on Mafia hierarchy, suggested that TOC entities are three conjoined entities: 1) producers of goods and services; 2) traffickers of the goods; and 3) overall TOC governance actors.[5] TOC governance exists to unify existing shadow economy structures in a similar fashion as a corporation would vertically integrate its supply chain. More specifically, TOC entities in Latin America have become polycrime entities,[6] embracing multiple types and forms of criminality. Increasingly, TOC entities are structured in such a way to encourage polycrime activity. This is particularly relevant to narcotraffickers, but is also applicable to other criminal entities for whom narcotics production, trafficking, and/or distribution are not their primary type of activity.[7] These entities now have decades of experience in illicit and illegal practices that benefit multiple different types of transnational criminal activity. With transnational networks in place, weapons trafficking, human trafficking and/or smuggling, intellectual property crime, counterfeit products, and counterfeit drugs all become viable productive activities.[8]

We suggest that there is a fourth role within TOC entities: the "violence worker." Violence workers are those members of TOC entities that use violence to enforce (bureaucratic) order. Violence workers appear organically, and become specialized, in the ranks of producers, traffickers, and governors, and work to reinforce TOC goals through the use of violence. The "order-enforcement" exercised by violence workers functions as a determined logic of coercion and violence aimed to define the extent of TOC governance.[9] Significantly, order-enforcement requires a substantial balancing act so that the fear constituted by TOC vio lence workers creates economic opportunities without fully dele-

gitimizing their standing, especially those that blend illicit and licit activities, or draws significant attention from state interventionary forces.[10] In other words, violence workers employ order-enforcement to normalize TOC entities' claims of legitimacy to govern and operate across their territories. As TOC entities grow and diversify, violence workers have become more indispensable.

For some organized criminal entities, violence workers mainly serve a productive role, meaning that they manage "strong arm" activities like extortion, protection rackets, burglaries, and robberies. In more sophisticated polycrime transnational organized criminal entities, violence workers commit similar activities, and involve violence specialization, like firefights (tiroteos), assassinations (asesinatos), and raids (incursiónes) at varying levels of intensity and tactical action, to ensure successful trafficking operations.[11] The economic gains from rudimentary violence work are rather insignificant compared with the funds received from successful trafficking operations. Moreover, varying levels and intensity of violence maintained by violence workers across all scales of TOC activity engenders a "criminal governance" that functions in opposition to and often in collusion with the state's capacity to govern, occupying an occluded space between everyday criminal (bureaucratic) activity and violent conflict.[12]

Borrowing from Mancur Olson's work, violence workers who support TOC entities are disinclined from participating in what Olson termed "roving banditry" because as "stationary bandits," they are economically successful and not raising the ire of state entities that could counter their efforts. However, when states flex their muscles and challenge TOC sovereignty, it incentivizes violence workers to organize against state forces and civilian populations to maintain the entity's existing business practices. Even though violence workers are indispensable to TOC entities in stimulating and maintaining illicit practices, (semi-) legitimate economic structures and individuals, so-called "facilitators", make TOC activities even more profitable by crossing the between the shadow economy and global economy to serve legitimate customers and TOC entities alike.[13] Facilitators serve wittingly, and sometimes unwittingly, to connect TOC entities to legitimate economic structures, like offshore bank accounts and shell corporations, in order to sustain growing polycrime infrastructures. Violence workers and facilitators both function to advance perpetuation of TOC activities and their profitability underpinning the foundations of the shadow economy.

Recent TOC Trends

In the past, TOC entities largely remained regional in their operational scope with strict hierarchical structures. Today, TOC entities are more variable and volatile embracing new, and often violent, operational strategies increasing not only their diversification of illicit activities, but also, the density of those illicit activities. Additionally, TOC entities increasingly engage in illicit activities that transgress territories and borders of a single state. This expansion poses serious threats to neighboring states and their citizens, generating both direct and indirect economic harm, affecting social structures, like public health, and hindering the development and stability of states.[14] Notable trends in TOC that present significant challenges today include:

1. Fragmentation: TOC fragmentation has led to increasingly adaptable, agile, and competitively violent criminal organizations with varying structures and wider networks.

2. Geographical expansion: TOC expansion has led to greater contestation over illicit inputs, routes, and markets globally.

3. Diversification: TOC entities are diversifying their criminal portfolios, thus increasing their criminal density, seeking greater profits, consolidation of markets, and safeguarded supply chains.

4. Legitimate entanglement: TOC entities are becoming increasingly entangled with legitimate businesses and actors, including state actors (e.g., corrupt security force personnel), and especially, banking institutions to launder money.

5. Specialization: TOC entities pursue cross-national specialization, forging networked criminal connections at regional and global scales.

6. Virtual: There is an increasing role of cyber capabilities in TOC as TOC entities exploit online dark networks (i.e., the dark web) and licit online economic platforms, to sell goods and services.

The most indelible issues we face when countering TOC involve the metastasizing and merging of regional entities into global juggernauts. The initial Medellín and Cali cartels were transnational because they produced their goods in Colombia and Bolivia and they were transported to, and sold in, the United States. Yet we have seen subsequent Mexican cartels— Sinaloa and Loz Zetas, for example—expand their reach globally partnering with European, Asian, Australian, and African organized criminal entities to reshape the drug trade.[15] This has been evident most recently in the mixing of Mexican

and European assets to produce highly refined crystal meth that has taken over the European recreational drug scene. In late 2020, police raids in The Netherlands discovered a professional crystal meth lab that was truly global: Mexicans cooked the meth using Dutch-made equipment and chemicals sourced from China. The recent raids have uncovered links to the Jalisco New Generation Cartel (CJNG), one of the newer and most violent Mexican cartels.[16] CJNG and the Sinaloa cartel have also been linked to the recent proliferation of fentanyl that has fueled the opioid epidemic in the United States over the last few years.[17] Cartels send envoys to China to purchase dual use precursor chemicals and/or bulk shipments of fentanyl, and then ship those to Mexican ports, like Lázaro Cardenas, where cartel members take possession of the material for further processing, trafficking, and then vending.[18] These methods, at the current economy of scale, make these operations incredibly profitable. The profitability and global nature have led to increases in violence brought about by difficulties managing the hierarchy across global space in addition to the opportunity to earn profit at all levels.

Conclusion

These characteristics of TOC entities—the increasingly global scope of their reach, the institutionalization of violence, and the fine line between illicit and illegal—have profound implications for the global economy. The implications of the capacity and capabilities to counter TOC profoundly shape if, when, and how these current and emerging trends continue to produce violent and destabilizing consequences. The growth in criminal density and geographical expansion of TOC entities across various regions in the world, including the U.S. Southern Border, will only continue to produce instability. As TOC entities form more sophisticated networks and means of transnational operation, it is necessary to consider ways to enhance data collection, analysis, and information sharing capabilities across states to keep pace with the rapidly changing dynamics of TOC activities, and to address gaps in policy and practice to counter TOC.

REFERENCES

[1] Gary, Ackerman, David Blair, Lauren Burns, Glen Butler, Hriar Cabayan, Regan Damron, Joseph D. Keefe, et al., *The 'New' Face of Transnational Crime Organizations (TCOs): A Geopolitical Perspective and Implications for U.S. National Security*, (Washington, D.C.: U.S. Department of Defense, March 2013).

[2] Leandro Medina, and Friedrich Schneider, *Shadow economies around the world: what did we learn over the last 20 years?*. International Monetary Fund, 2018.

[3] Chamber of Commerce (ICC) and International Trademark Association (INTA), *The Economic Impacts of Counterfeiting and Piracy,* 2017. https://iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf

[4] Medina, L., & Schneider, F. (2021). The Evolution of Shadow Economies through the 21st Century. *The Global Informal Workforce*, 10.

[5] Radio Interview with Federico Varese, *KYMN*, August, 11, 2021. https://kymnradio.net/2021/08/11/national-security-this-week-with-professor-federico-varese-8-1-21-transnational-organized-crime-networks/

[6] Time Hall, *The economic geographies of organized crime* (New York, NY: Guilford Publications, 2018).

[7] Organized Crime Drug Enforcement Task Force, U.S. Department of Justice, *FY2017 Interagency Crime and Drug Enforcement Congressional Submission*, 2017.

[8] Organized Crime Drug Enforcement Task Force, U.S. Department of Justice, *FY2017 Interagency Crime and Drug Enforcement Congressional Submission*, 2017.; European Union Intellectual Property Office, EUROPOL, *IP Crime and its link to other serious crimes: Focus on Poly-criminality*, 2020.

[9] Samuel D. Henkin, *Geographies of Non-Lethal Weapons: Transformative Technologies and Political Violence*. Dissertation. University of Kansas, 2019.

[10] David Carnevale, Criminal humanitarianism: A visual exploration of criminal legitimisation, between alternative moralities and the political vacuum, *Interdisciplinary Political Studies*, 4(2) 2018: 79-125.

[11] Graham H. Turbiville Jr. Firefights, raids, and assassinations: tactical forms of cartel violence and their underpinnings, Smal Wars & Insurgencies, 21(1) 2010: 123-144.

[12] Benjamin Lessing, Conceptualizing Criminal Governance, *Perspectives on Politics*, 19(3) 2020: 854-873.

[13] U.S. National Security Council, *Strategy to Combat Transnational Organized Crime. The White House*, 2011, https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime

[14] Frank Madsen, *Transnational organized crime* (New York, NY: Routledge, 2009).

[15] Diorella Islas. "The process of transnationalization of drug trafficking organisations: the case of the Mexican cartels." PhD diss., University of Bath, 2020; Anthea McCarthy-Jones, Caroline Doyle, and Mark Turner. "From hierarchies to networks: The organizational evolution of the international drug trade." *International Journal of Law, Crime and Justice* 63 (2020): 100436.

[16] Valentina Pop, "Meixcan Cartels Are Now Cooking Chinese Chemicals in Dutch Meth Labs," *The Wall Street* Journal. 8 December, 8, 2020.

[17] Steven Dudley, Deborah Bonello, Jaime López-Aran-

da, Mario Moreno, Tristan Clavel, Bjorn Kjelstad, Juan José Restrepo, *Mexico's Role in the Deadly Rise of Fentanyl,* The Wilson Center's Mexico Institute and Insight Crime. February 2019.
[18] Jude Webber, "Mexican Drug Cartels See Big Profits in Fentanyl," *Financial* Times, April, 27, 2021.

AUTHORS

Marcus A. Boyd is the graduate studies director and head of geospatial analysis at the National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland, where he oversees research relating to terrorism, illicit finance, and GIScience

Samuel Henkin is a senior faculty specialist and Geospatial Research Unit researscher at the National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland, where he focuses on the study of political violence, instability, and conflict.