CYBERSPACE & OPEN EMPOWERMENT IN LATIN AMERICA

Across Latin America, cyberspace is fundamentally rewiring the ways groups, individuals and states engage with politics, economics, social action and governance. With some 40% of the population now online, connectivity is expanding faster than in any other part of the world. Most of that expansion is happening amongst the young – digital natives with ambitions to change and better their lives.[1] Civil society has also moved online, evidenced in a groundswell of blogs and networked social movements such as *YoSoy132* and *Blog del Narco*. The recent street protests in Brazil may signal a new popular *awakening*, as digital natives flex their collective political muscles.

Criminals are also rapidly colonizing Latin American cyberspace, as evidenced in the stark rise in cyber-enabled criminality. The regional narco-economy and associated gangs use online platforms to organize and advertise their activities, recruit members, intimidate authorities and citizens, extort money and hire contract killers.[2]

Across it all, states are struggling to cope. Government responses vary widely. Most involve a complex mix of leveraging cyberspace to enhance governance while adopting cyber-security policies, laws and capabilities to police and impose order on this promising, risk-filled and volatile space.

The Open Empowerment Initiative (OEI) investigates how cyberspace is shaping citizen action and state-society relations in Latin America. This note summarizes preliminary findings from field research in Argentina, Brazil, Colombia, El Salvador, and Mexico, as well as implications for the Organization of American States (OAS).

KEY IMPLICATIONS FOR THE OAS:

- **A broader approach to cyber-security is needed.** The causes and effects of cyber-security challenges cannot be reduced to narrow technical and institutional reform issues. The OAS' Secretariat of Multidimensional Security could broaden its approach to account for the multi-faceted ways in which cyberspace is generating positive and negative forms of empowerment.
- **Shared situational awareness matters.** The dynamics and characteristics of cyber-threats and cyber-responses in Latin America vary across states, sub-regions, cities, and even neighborhoods. The OAS should seek to bolster its abilities to monitor change, from a broad to granular scale, and disseminate information on a routine basis.
- **Coordination is a key to success.** The cyber-security challenge is multi-dimensional, and so are effective responses. Close and continuous coordination between states, the private sector and civil society is the new normal for organizations such as the OAS's Secretariat of Multidimensional Security.

[1] The young are connecting, with over two-thirds of Latin America's online population under the age of 35. Social media is especially popular amongst youth and Argentina, Brazil, Colombia, and Mexico are in the top 10 countries worldwide for time on social media.
[2] See, for example, *Facebook Hitman Highlights Organized Crime Online Presence*. http://m.insightcrime.org/pages/article/4238

OPEN EMPOWERMENT IN LATIN AMERICA: SOCIETAL PATTERNS AND TRENDS

The social impact of cyberspace empowers all actors in Latin America. Ideas – much like trade – spread across borders in Latin America within a cyber-ecosystem. Digital natives from across the region are building on their shared culture, history, language, and interests. This is having an impact. The lessons of successful social and political mobilization are being learned and imitated throughout the region via cyberspace. Brazil's recent street protests illustrate the point. Lessons are also being absorbed by criminal gangs and armed groups, particularly those involved in the global narco-economy. Overall, politics is being transformed at the local level, as cyberspace enables change that scales faster than state authorities can respond. As the institutional order struggles to adapt, the cumulative impact of these shifts could be fundamental and enduring.

Cyberspace mirrors inequalities and exacerbates real-life conflicts. Throughout the region, citizens tend to be ahead of the state in recognizing the potential of cyberspace for satisfying their interests and pushing for change. However, in countries where inequalities are most stark, access to new technologies by the disenfranchised can also be compromised. Extreme shortcomings in governance and socio-economic well-being tend to be reproduced online. The OEI finds that these patterns are significant not just between states, but also within them. It suggests the need for targeted interventions in regions where digital and socio-economic weaknesses persist.

Cyberspace empowers crime, and criminal groups. Outpacing authorities and civil society, criminal actors have deftly exploited cyberspace's *open empowerment*. Across the region, conventional crime is going digital, as narco-cartels and drug dealers, gang members, human traffickers and others harness the power of the web to organize operations, intimidate competitors and others, seek recruits, flaunt state controls, extort money and sell their wares. Increasingly, criminals use mainstream social media, such as Facebook, Orkut and SilkRoad to sell illegal drugs. Indeed, some groups, fueled by "narco revenue," have built and maintain their own sophisticated telecommunications networks. An absence of appropriate legislation and capabilities leaves authorities unable to effectively police online spaces. Moreover, in some countries armed criminal groups dominate and surveil cyber spaces, to impose silence around their activities. The effort has been effective, stifling civic journalism and engagement, media reporting, and even democratic governance.

There are many risks associated with *open empowerment* in Latin America, not least to the newly empowered. The rise of citizen activism online has attracted blowback from both goverments and criminal groups. Even as they press for political change, denounce corruption and criminality, and express social grievances, Latin Americans have suffered new forms of suppression – both online and off. The very opportunity to mobilize for change has also opened up new forms of exposure and vulnerability, leading student and activist groups to develop new forms of protection and anonymity. On some occasions, citizen groups have developed innovative strategies, often leveraging cyber-space, to meet these new threats. In other cases, civic action groups have been forced to accept information black-outs, resulting in acute forms of censorship.

OPEN EMPOWERMENT: STATE RESPONSES

Across Latin America, governments have been struggling to keep up with the pace and range of cyber-enhanced change. Most recognize the array of opportunities and risks for governance, democratic development, law and order, and security. Unlike in North America, Europe, and parts of Asia, however, governments and private sector entities in South and Central America are less preoccupied with issues of cyber-war or cyber-terrorism and more focused on cyber-mediated crime such as e-banking scams, money laundering, drug trafficking and child pornography. Latin American governments are only beginning to adopt laws, institutions, and countermeasures to combat online criminality.

State responses to cyberspace tend to align with their responses in other sectors. States with legacies of military rule tend to securitize responses to cyber empowerment. In the cases of Argentina and Brazil, for example, public security agencies – both the armed forces and the police – are imposing more control over the governance of cyberspace. El Salvador and Mexico, by contrast, tend to adopt more sporadic responses, giving rise to grey spaces in the regulation of the cyber commons. In states with high fragility and limited resources, the state tends to take a backseat, as citizen action groups and others – including powerful criminal groups – assume more dominant roles.

At a regional level, cyber-security efforts are being coordinated through the OAS and include harmonizing national legislation and adopting the Comprehensive Inter-American Strategy to Combat Threats to Cyber-Security. But Latin American countries are also starting to adopt new legislative frameworks, create specialized law enforcement agencies, and form Computer Security Incident Response Teams (CSIRTs). There is also talk of engaging more comprehensively with cyber-threats through sub-regional mechanisms including the Union of South American States (UNASUR), the South American Common Market (Mercosur) and others, though concrete actions are lagging.

Latin American civil society plays a major – if still comparatively under-valued – role in cyber-security governance. Owing in part to the decentralized character of cyberspace, the private sector is in some cases far ahead of governments in assessing cyber-threats and formulating responses, particularly in relation to the banking and e-services sectors. Meanwhile, internationally, a number of non-governmental entities actually control systemic features of cyberspace such as the allocation of internet domain names. Notwithstanding its comparative strengths and real exposure to cyber-threats, the private sector is still punching below its weight when it comes to promoting cyber-security across Latin America.

OPEN EMPOWERMENT: CASE STUDIES

ARGENTINA

Many of Argentina's cyber empowerment issues echo those encountered in more established economies such as in North America and Western Europe. In the past few years, cyberspace has enabled massive social and political protests, which have brought together a wide range of groups quickly, easily, and in an organized fashion. Cyberspace is rivalling traditional institutions such as political parties, unions, and public entities. Not surprisingly, traditional politics are starting to adapt to the new imperatives of the digital age. A new party called La Red ("The Network") was created based on the principles of electronic democracy and digital citizen participation.

When it comes to crime, Argentina exhibits one of the richest and most diversified cyber-crime environments in the world. Meanwhile, the government appears to have pursued extra-legal controls of its citizenry online.This was sharply highlighted by the emergence in February 2012 of *Proyecto X*, a plan intended to illegally spy on and monitor citizen movement leaders.

BRAZIL

Cyberspace represents a policy area where emerging countries like Brazil can make a notable impact around the world and domestically. Troublingly, the preoccupation with soft power projection abroad may distract Brazilian investments in addressing real and present cyber-threats faced by its citizens. At the grassroots level, cyberspace is amplifying ostensibly geographically-remote grievances that seldom come to the attention of elites in the capital cities. Moreover, digital activism is increasing and shows some promise to bring about political change, as demonstrated in Brazil's recent street protests. And while it seldom translates into real power, the case of Brazil may prove an important exception.

Even so, Brazil has the highest level of cyber-crime in Latin America and ranks amongst the worst affected globally. This is especially the case when it comes to fraud, identity theft, money laundering, and other online crimes. And while the country and its businesses suffer from comparatively few cyber-attacks from abroad, Brazilian hackers are reportedly committing growing numbers of offenses in Portuguese- and Spanish-speaking countries and communities. The risks of increasingly securitized responses from the Brazilian military are very real.

COLOMBIA

After years of lagging behind civic activists, Colombia's politicians and public officials are now taking the lead in cyberspace. Colombian authorities have become more cognizant of how cyberspace represents a new area of operation, particularly in relation to armed groups, both guerrilla and paramilitary. Colombian legislative politics were shaken-up by the advent of grassroots activists that used ICTs, including the Green Party in 2010. Colombians are also increasingly leveraging ICTs to protest the country's long-running civil conflict. The "One Million Voices Against the FARC" movement started on Facebook in 2008 and led to unprecedented demonstrations, drawing out some 10 million street protesters.

At the same time, Colombia's economically-driven criminal groups are also migrating their operations online. Though not necessarily amounting to a "revolution" in organized crime, such a change has meant an amplification of conventional criminal practices. Not surprisingly, cyber-security has entered official government discourse and the government is adopting increasingly securitized and militarized approaches that could have implications for privacy and freedoms online and off.

EL SALVADOR

Even in poorer, low connectivity countries like El Salvador, the impact of cyberspace is major and widespread. The El Salvador case provides a window into trends we can expect to see in other poorer countries that come online. Citizen movements with clear political objectives are mobilizing online and successfully managing to bring about policy changes. Moreover, for the first time the Diaspora will be able to vote online in the 2014 presidential elections. Notwithstanding these events, major change appears for now to be beyond the reach of online citizen movements.

Cyberspace in El Salvador is also enhancing criminal activities and reach. Criminals have systematically exploited cyberspace to profile individuals, creating a database to support extortion activities. Gangs such as MS-13 and M-18 are turning to cyberspace to recruit followers and leverage social media and other mechanisms for surveillance, extortion, and coercion.

MEXICO

In Mexico, technological empowerment has allowed citizens to engage proactively in social and political action, and to satisfy their needs for information and security without the support of public authorities. Mexico also showcases examples of collaborative government-citizen e-initiatives to respond to violence and crime. For example, the *Centro de Integración Ciudadana* (CIC) in Monterrey draws on crowdsourcing to promote targeted public security responses.

The Mexican case study also illuminates how powerful actors (whether criminal or political) are enforcing new forms of censorship. Drug cartels, for example, regularly intimidate, extort and kill hacktivists and bloggers. This has led to a widespread cooling effect on conventional and social media use by citizens. At the same time, the public exhibits a thirst for *narco corridos* (music that glorifies narco-culture), which have spread rapidly due to popular demand online, despite government attempts at censorship.

ABOUT THE OPEN EMPOWERMENT INITIATIVE

Against the backdrop of Brazil's cyber-empowered street protests or the online dimensions of Mexico's Drug War, the Open Empowerment Initiative (OEI) investigates how cyberspace is shaping citizen action and state-society relations in Latin America. OEI research considers:

- How digital natives are leveraging cyberspace to pursue political, social and economic empowerment;
- How cyber-empowered actions are shaping state-society relations, and security; and,
- How governments are responding.

Local researchers are exploring these questions in Argentina, Brazil, Colombia, El Salvador, Mexico, and the region as a whole. In addition, advanced cyber analytics are being deployed to develop a better understanding of Latin America's social media environment and its emerging societal resonance. The OEI is a partnership between The SecDev Foundation (Canada) and The Igarapé Institute (Brazil). The initial phase of research (2012-13) is supported by Canada's International Development Research Centre. For more information visit openempowerment.org

ABOUT THE IGARAPÉ INSTITUTE

The Igarapé Institute is a southern think tank focused on promoting evidence-based alternatives on drug policy, violence reduction and international cooperation in Brazil, but also across Latin America and around the world. The Institute focuses on generating informed debate through research on emerging issues spanning the security-development continuum. The Institute has an international profile having undertaken intensive policy and field-based assessments in partnership with the Brazilian, Canadian, Norwegian, Swiss and UK governments, Google Ideas, the Bernard Van Leer Foundation, Open Society Institute (OSI), International Development Research Center (IDRC), and various multilateral, bilateral and private sector groups. For more information visit www.igarape.org.br.

ABOUT THE SECDEV FOUNDATION

The SecDev Foundation supports research and programming at the cross-roads of global security and development. We work with local stakeholders in countries and regions at risk in Asia, Africa, Eurasia, the Middle East and Latin America. We leverage advanced cyber analytics to extend and empower local knowledge and resilience in the face of emerging risks. We engage across three areas: cyber-empowerment; emerging sources of security and resilience; and armed violence prevention and reduction. The Foundation is a Canadian-based, not-for-profit organization, whose work is supported by the International Development Research Centre, the US State Department's Bureau for Democracy, Rights and Labor, The Open Societies Foundation and Freedom House.

This work was carried out with the aid of a grant from the Canadian International Development Agency and the International Development Research Centre, Ottawa, Canada

TheSecDev FOUNDATION

World Exchange Plaza, Suite 1150,
45 O'Connor Street, Ottawa, Ontario,
Canada, K1P 1A4

IGARAPÉ INSTITUTE

Rua Visconde de Caravelas, 111 Botafogo,
Rio de Janeiro – RJ – Brasil
22271-041

IDRC | CRDI Canada