A fine balance:

Mapping cyber (in)security in Latin America

Igarape Institute and The SecDev Foundation[1]

Latin American governments are worried about criminality in cyberspace. This is hardly surprising. Like all regions around the world, Latin America is experiencing an information revolution. Intriguingly, Latin America has not witnessed the equivalent of an Arab Spring or the Occupy movements that flared up across the Middle East, North America and Western Europe between 2010 and 2011. Rather, Latin America´s information *revolución* is reinforcing already high crime rates and is being driven by some common factors. On the one hand, the region features a youthful population craving more online access, with almost two-thirds of all internet users under the age of 35. Likewise, internet usage is growing more rapidly than virtually anywhere else in the world: more than 40 per cent of the population is online. Latin America also registers amongst the highest rates of growth in mobile devices, especially smartphones. Combined with shared language(s) and culture(s) spanning the Americas, it is little wonder that Latin Americans are the most voracious consumers of social media on the planet.

Latin America´s cyber-crime problem is a direct consequence of the exponential growth of cyberspace across the region. Indeed, the internet and related social media tools have not just empowered citizens to exercise their rights, but also enabled and extended the reach of gangs, cartels and organized criminals. Predictably, governments, private sector and civil society groups across Latin America have stepped up their responses to contain and manage the threat. These encompass legislative measures, specialized agencies, directed research programs, professional exchanges, and expanded international cooperation. Yet progress in preventing and reducing online criminality is itself hampered by an absence of internationally accepted definitions of what exactly constitutes "cyber-crime," the weak capabilities of law enforcement agencies, and the complex forms and scale of crime online.

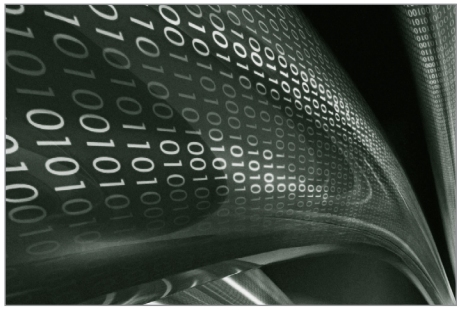
---

1 This Strategic Paper is the first in a series that will examine the intersection of new media, cyberspace and empowerment across Latin America and the Caribbean. The Strategic Paper was authored by Gustavo Diniz and Robert Muggah, with additional input from Rafal Rohozinski and Elinor Buxton. This Paper was carried out with assistance from the International Development Research Centre (IDRC) in Ottawa, Canada.

This **Strategic Paper** examines the character and dynamics of cyber-crime and the ways in which it is being addressed in Latin America. A particular focus is on what might be described as "new criminality" emerging in cyberspace – organized criminal hacking, identity theft, advanced credit card fraud and online child exploitation. The Paper draws on a review of the public and grey literature from more than thirty countries and interviews with dozens of experts across the sub-continent to shed light on the present cyber-security and cyber-defence architecture being erected in Latin America. Overall, it finds that Latin America exhibits a heterogeneous landscape when it comes to cyber-crime. And while all countries have witnessed a surge in cyber-crime, threats and responses tend to be clustered in specific countries, such as Argentina, Brazil, Chile, Colombia, Cost Rica, the Dominican Republic and Mexico, where online populations and internet penetration rates are highest. This **Strategic Paper** finds that:

- **Latin American governments are only beginning to adopt laws, institutions and countermeasures to combat online criminality:** At a regional level these efforts are being coordinated through the Organization of American States (OAS) and include harmonizing national legislation and adopting the *Comprehensive Inter-American Strategy to Combat Threats to Cyber-Security*;
- **Latin American country responses to cyber-crime are increasingly aligned:** Most Latin American states are pursuing a 4-pillar strategy that includes: (i) the adoption of relevant legal frameworks; (ii) the creation of specialized law enforcement agencies; (iii) the formation of Computer Security Incident Response Teams (CSIRTs); and (iv) the establishment of specialized units within the executive branch of government;
- **Latin America´s civil society plays a major – if under-valued – role in cyber-security governance:** Due to the decentralized character of the internet and overlapping forms of horizontal collaboration, civil society is in some cases far ahead of governments in assessing cyber-threats and formulating responses. Internationally, a number of non-governmental entities actually control systemic features of the worldwide web such as the attribution of domain names; and
- **Notwithstanding its comparative strengths and real exposure to cyber-threats, the private sector is less engaged in promoting and engaging in cyber-security across Latin America:** Many larger corporations in the banking and services sectors are non-transparent about the scale of the threats they are facing. Owing to their desire to avoid loss in market share, they typically adopt low-key, periodic, and restricted actions. By contrast, companies involved in information technology manufacturing and services markets are more involved in supporting digital platforms designed to raise awareness.

The **Strategic Paper** proceeds in several sections. The first section considers the conceptual gap which frustrates coherent approaches to addressing cyber-crime. While few experts dispute the risks presented by new forms of online



"The internet has not just empowered citizens to exercise their rights, but also enabled and extended the reach of gangs, cartels and organized criminals"

criminality, there are no accepted definitions of cyber-crime, making it difficult to harmonize legislation and pursue investigations requiring transnational cooperation. Section two reviews the scale and dimensions of cyber-crime in Latin America, focusing primarily on the so-called new criminality. The third section provides a general review of regional approaches to containing cyber-crime, including legal conventions, guidelines and emerging practices, while Section four examines the operational responses of governments, private sector and non-governmental organizations. The final section offers some concluding reflections on future research directions.

"Cyber-crime includes those activities in which computers or networks are employed as tools, targets or places for the achievement of criminal ends"

Cyber-crime: a definitional gap

Controlling cyber-crime is challenging no matter how robust and sophisticated a state or citizen's response mechanisms. The protection against insecurity in cyberspace is – or at least it should be – a global concern. The interconnectedness of societies and markets and increasing reliance on information communication technologies (ICTs) is perhaps the primary motive for public and private actors to formulate laws and increase their capabilities to police cyberspace. Any large government or corporate bureaucracy, for instance, features an IT department responsible for establishing virtual protection systems. Likewise, private users are constantly required to manage anti-virus and malware software in their personal devices. Yet the knowledge base about the extent of cyber threats is comparatively limited and dispersed. This is due in part to the novelty of the issue. It is essential, then, that there be some basic consensus on terminology, particularly when considering the variation of languages in Latin America.

There is comparatively little agreement on the basic nomenclature of cyber-crime. The International Telecommunications Union (ITU), a standard-setting agency, describes cyber-crime as "those activities in which computers or networks are employed as tools, targets or places for the achievement of criminal ends." But this definition is too broad to be meaningfully applied or operationalized. Meanwhile, the Council of Europe's *Convention on Cyber-crime* divides cyber-crime into four dimensions:

- offences against the confidentiality, integrity and availability of computer data and systems (e.g. hacking, phishing, espionage, interception, interference);
- content-related offences (e.g. child pornography, hate speech, gambling, libel, spam);
- computer-related offences (e.g. fraud, forgery, identity-theft, laundering); and

- copyright and trademark-related offences (file sharing).[2]

But even here, it is difficult to narrow down such crimes since most tend to be complex or combined and span multiple categories (e.g. phishing, cyber-terrorism or even hacktivism). Complicating matters further, attributed crimes inevitably vary from country to country.

The absence of a comprehensive and consensus-based framework for legislating on cyber-crime has resulted in a global patchwork of responses and loopholes open to exploitation. Part of the problem relates to the idiosyncratic nature of cyber-crime itself, which is exceedingly difficult to isolate. Indeed, cyberspace has an empowering effect for what might be described as "old" crime groups by allowing them to bypass borders anonymously and with ease. It is hardly surprising, then, that across Latin America cyberspace is being exploited by drug cartels and youth gangs.[3] But as dangerous as these groups may be, it is also important to recall that almost 2 billion people worldwide are internet users and that there are almost 6 billion cell phone subscriptions with most core networks largely under-protected from all manner of predatory criminals. Indeed "computer and internet users are often the weakest link and the main target of criminals. It is often easier to attack private computers to obtain sensitive information, rather than the well-protected computer systems of a financial institution."[4]

"Almost 2 billion people worldwide use digital devices and networks and are under-protected from cyber-crime"

Alongside cyber-crime, another term that has emerged internationally, but also in Latin America, is hacktivism. The expression was popularized by the so-called Anonymous group – a decentralized online community acting in a coordinated manner towards a commonly agreed goal. However, the term itself was first coined in 1998 by an underground group[5] to indicate a direct action in a digital environment to affect political change. The expression combines "hacking" with "activism" and thus integrates what might be interpreted as cyber-crime activity using the above-mentioned categories with political mobilization. Yet the fact that hacktivist activities may result in identity theft or involve illegal activities – even in the service of what might be described by some as progressive social outcomes – means that most governments categorize such activities as criminal.

2 TheITU does not consider this typology completely adequate since "it is not based on a sole criterion to differentiate between categories". While 1, 2 and 4 focus on the object of legal protection, 3 refers to the method used to commit the crime. See ITU, 19 at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed March 01, 2012).

3 See Ungerleider, N. (2011) "Mexican Narco-gangs War on Digital Media", *Fast Company*, June 10. http://www.fastcompany.com/1785413/narcogangs-social-media-and-21st-century-crime. Also consult Gutierrez, R. (2012) "Leaking Secrets, Leaking Blood", *Boing Boing Special Feature* at http://boingboing.net/2010/09/14/narco.html#previouspost.

4 See ITU, 85.

5 The group was called the Cult of the Dead Cow (cDc). The cDC claim that they promoted technology-driven advocacy to foster human rights and the open exchange of information.

Other types of cyber-threats that are routinely invoked around the world include cyber-terrorism and cyber-warfare. While not considered a major threat in Latin America, cyber-warfare refers to politically motivated actions deployed by governments in order to penetrate another state´s computer networks for the purposes of causing damage and destruction.[6] Cyber-espionage can be one fo the means or ends of cyber-warfare, though the characterization becomes more complex when considering the involvement of nationally owned or private corporations involved in industrial espionage. While the goals of cyber-terrorism may be the same as cyber-warfare, the difference is that it is perpetrated by non-state actors.[7] As with the label terrorism more generally, the term is controversial. Indeed, many of the above-mentioned cyber-crime characteristics could be interpreted as cyber-terrorism.

Scope and scale of cyber-crime in Latin America

There is growing recognition of the extent of cyber criminality across Latin America. Unlike in North America, Europe and parts of Asia, governments in South and Central America are less preoccupied with issues of cyber-war or cyber-terrorism than with criminal practices of individuals and crime networks connected to cyberspace with the intention of making illicit economic gains. Common examples range from e-banking scams to drug trafficking and child pornography. Moreover, as discussed below, there is a growing preoccupation with hacktivist groups targeting official institutions and agencies with the intent of expressing political and social grievances. Such activities entail the closing down of official websites of government bodies and private sector entities and, in some cases, the theft of ostensibly confidential information, though not with the express purpose of economic gain.

Predictably, the rapid increase in connectivity to the internet in Latin America over the past decade has increased the overall volume and exposure to associated cyber threats. Over the past decade the number of internet users in South America has increased tenfold (1,111 per cent) and fifteen times in Central America (1,480 per cent). By 2011, internet penetration in South America and Central America reached 43 per cent and 32.6 per cent of the population respectively (see Annex 1).[8] Likewise, 3G mobile phone subscriptions also increased tenfold across Latin America during the same period.[9] Indeed, Latin America registered amongst the highest rate of growth in mobile services globally.[10]

6 See Clark, R. (2010) *Cyber War: The Next Threat to National Security and What to Do About it.* New York: Harper-Collins.

7 See Security and Defense Agenda (2011) *Cyber-Security: The Vexed Question of Global Rules* (Brussels), 16-17.

8 Although internet penetration in LAC is still below the rates of North America (78.6 per cent) and Europe (61.3 per cent), it is far above the African and Asian average percentages (13.5 per cent and 26.2 per cent).

9 According to ITU data, between 2000 and 2010, in LAC region there was an average increase of 10 times in the number of mobile phones in the hands of its citizens. Countries like Antigua and Barbuda, Bahamas, Argentina, Brazil, Chile, El Salvador, Honduras, Jamaica, Panama, Suriname, Trinidad and Tobago, and Uruguay even have more than 1 mobile phone per inhabitant. Internet World Stats, http://www.internetworldstats.com (accessed April 19, 2012).

10 While behind Africa and Asia, Latin America was ahead of Europe and North America. Indeed, shipments of smartphones grew by over 117 per cent in 2010. Industry analysts predict that by 2016 smartphones capable of accessing high-speed Internet will account for over 50 per cent of all cell phone sales in the region.

"Over the past decade the number of internet users in South America has increased tenfold (1,111 per cent) and fifteen times in Central America (1,480 per cent)"

Latin America´s particular demographic profile has contributed to this explosive growth in internet penetration. The region´s user-base is disproportionately youthful when compared to other regions, with close to two thirds of its users under the age of 35, compared to a little over half globally. What is more, Argentina, Brazil, Chile, Peru, Colombia, and Mexico are amongst the top ten countries with populations spending the most time on social networks.[11] Such countries are thus home to large populations of digital natives – young people who easily navigate the net and increasingly migrate their day-to-day transactions there. At the same time, there has been a progressive virtualization of key private commercial activities including e-banking and e-commerce in Latin America. While there are no readily available statistics on the overall volume of usage across the region, some countries provide an indication of the scale of economic transactions.[12] For example, in Brazil, e-commerce has grown from USD 250 million in 2001 to more than USD 9 billion in 2011.

The expansion in cyber penetration, increase in e-service provision and the growth in young digital newcomers has resulted in a higher exposure to cyber-crime. Yet notwithstanding overall regional increases in internet use, the incidence of cyber-crime is highly uneven across countries. Specifically, middle- and upper-income countries with more ICTs – both in terms of higher internet usage and more mobile phones – such as Argentina, Brazil, Chile, Colombia, Costa Rica, Dominican Republic and Mexico, are the primary targets of cybercriminals, most of whom operate within Latin America. It should also be stressed that there is a digital divide in Latin America which shapes the extent of cyber-crime. Specifically, some countries such as Belize, Bolivia, Cuba, Nicaragua and Guatemala have fewer than 20 per cent of their populations connected to the internet. The variation in exposure and vulnerability goes some way to explaining why there is an uneven spatial concentration of cyber-security initiatives in the region.

The most widespread types of cyber-crime across Latin America appear to be related to the first category noted above, namely offences against the confidentiality, integrity and availability of computer data and systems. The use of "phishing" – the use of misleading digital tools such as fake webpages and intrusive applications to access confidential data – is widespread. The use of malicious software such as trojans, worms and spyware is also increasingly common. While the costs are not widely publicized, some specific examples are illustrative. For example, in the first trimester of 2011, banking fraud on its own is estimated to have led to costs of USD380 million from Brazilian banks alone.[13] According to a limited sample of Latin American countries compiled by Kaspersky Labs (2011), at least 20 malicious malware programs were detected in the past few years, including those designed to steal e-banking passwords, pin codes and credit card

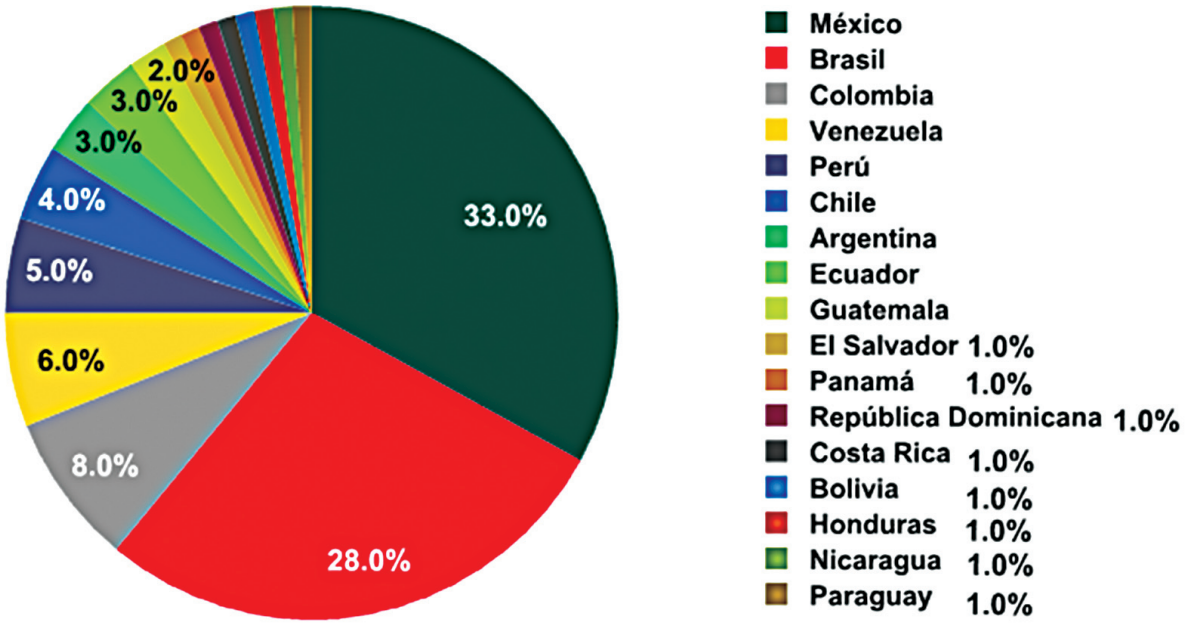
11 See ComScore (2012) *Futuro Digital – Latinoamerica 2012*, March.

12 See Econsultancy Digital Marketers United (2012) *Internet Statistics Compendium*.

13 See http://www.cyber-warzone.com/cyber-warfare/brazil-prepares-cyber-war (accessed April 19, 2012)

information across Latin America (see Figure 1).[14] The most common types were malware packages designed to appear as "legitimate" sites requesting personal data from users, but it also includes infection through the use of USB devices and social networks. Email scams, however, are increasingly less frequent.

Figure 1. Distribution of victims of malware across Latin American countries (2012)[15]



Another growth area in relation to cyber-crime in Latin America relates directly to drug trafficking. The net has emerged as a critical interface in the selling and purchasing of all manner of commodities, including both prescription and illicit narcotics. In Brazil a wide assortment of drugs are openly sold on popular social network sites such as Orkut and Facebook. Likewise, drug profits are often laundered through the internet through the purchasing of goods and services and the transferring of cash. Meanwhile, major cartels in Colombia and Mexico are mobilizing on the net in order to intimidate, signal control over territory, and extract illicit rents. The digital domain allows them to project influence and multiply their distribution networks, in some cases publicly challenging municipal and district level authorities.[16] As has been amply shown from Ciudad Juarez to Medellin, such groups also use the internet to threaten and silence civil society, particular journalists, bloggers and activists.[17]

14 The most commonly reported types of malware included Trojan.Win32.Generic (14%), DangerousObject.Multi.Generic (12%), and Net-Worm.Win32.Kido.ih (7%).

15 See Bestuzhev et al. (2012) *Panorama viral de América Latina en el 2011 y los pronósticos para el 2012*. Available at: http://www.viruslist.com/sp/analysis?pubid=207271158.

16 See Sullivan, J. and Elkus, A. (2012) *Mexican Drug Lords vs. Cybervigilantes and the Social Media*. March. Available at: http://mexidata.info/id3288.html (accessed April 11, 2012).

17 See Ungerleider (2011).

There are also concerns that more traditional street gangs across Central and South America – often in collusion with Latino gangs in the US – are migrating online.[18] This coincides with fears of so-called third generation and transnational gangs that are believed to be operating from California and Sinaloa to Tegucigalpa and Medellin.[19] Latin America is not alone in this regard: Interpol recently reported that upwards 80 per cent of all global online crime is now connected to organized gangs operating across borders.[20] There is also a surge in social media reporting on the mobilization of criminal gangs and cartels, not least the spectacularly popular internet site, Blog del Narco.[21] Yet it appears the involvement of organized gangs on the net is growing more intractable, not less. Criminal groups from Latin America are also learning from more experienced cybercriminals in Eastern Europe. And at the epicenter of this growth industry is Brazil – a country that routinely features in the top ranking of cyber-crime across Latin America.[22]

"Upwards of 80 per cent of all global online crime is now connected to organized gangs operating across borders"

Alongside more conventional cyber-crime is a recent increase in more politicized forms of cyber-criminality. In contrast to internet activism, hacktivism is generating a host of challenges to public and private actors alike. The key means tend to include *denial-of-service attacks* (DoS) or *distributed denial-of-service attacks* (DDoS) that can shut down institutional websites for extended periods and limit access to key resources to intended users.[23] Another common practice relates to stealing confidential information from designated authorities and institutions with the goal of making it available to the general public or extracting concessions. A difficulty in addressing hacktivism is that the political agendas of its proponents are often opaque and vary from group to group, many of whom are highly dispersed and exhibit dynamic membership structures. Two key groups – Anonymous and LulzSec – are especially common in Latin America and have been involved in launching DoS and DDoS attacks on governments, private corporations and banks.[24]

18 See Wilson, T. (2011) "Latin America´s Criminal Gangs Get Tech-Savvy", *InSight Crime*, December 14. http://insightcrime.org/insight-latest-news/item/1976-latin-americas-criminal-gangs-get-tech-savvy.

19 Muggah, R. (2012) "The Transnational Gang: Challenging the Conventional Narrative", in Shaw, T., Grant, T. Cornelissen, S. Eds. *The Ashgate Research Companion to Regionalisms*. Burlington VT: Ashgate.

20 See Weizman, S. (2012) "Interpol Says Organized Gangs Behind Internet Crime Boom", *AFP*, May 8. http://ca.news.yahoo.com/interpol-says-organised-gangs-behind-internet-crime-boom-204448909.html.

21 See http://www.blogdelnarco.com/.

22 See, for example, the *Norton Cyber-crime Report* at http://www.symantec.com/content/en/us/home_homeoffice/html/ncr/ and the *Symantecloud Report* at http://www.symanteccloud.com/globalthreats/overview/r_mli_reports?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Oct_worldwide_intelligencereportoct2011.

23 Malicious software is also frequently deployed to carry out these types of hacking activities.

24 See http://latimesblogs.latimes.com/laplaza/2011/06/hacking-brazil-latin-america-mexico-lulzsec-petrobras-1.html (accessed April 15, 2012).

A number of high-profile instances of hacktivist attacks have drawn attention to their potentially destabilizing effects. In 2011, for example, the Peruvian and Chilean governments were threatened by Anonymous in response to their declared efforts to monitor social networking activity. The hacktivist group called its operation Andes Libre (Free Andes). That same year, Anonymous also announced that it would attack Nicaragua and Venezuela for their overt support of Muammar Muhammad Gaddafi's regime in Libya. It should be noted that in contrast to the majority of cyber-crime noted above, hacktivist groups appear not to be based exclusively or even primarily in Latin America. For example, a coordinated series of cyber-attacks were directed against the Colombian Ministry of Defense, presidential websites, Chile´s ENDESA electricity utility, the national library and other targets in 2011 and early 2012. During the Interpol-led *Operation Unmask* – a major intervention coordinated with law enforcement agencies from Argentina, Chile, Colombia and Spain in February 2012 – the 25 arrested hackers were widely distributed around the world.

Regional responses

The principal international instrument for mobilizing state responses to cyber-crime is the Council of Europe´s *Convention on Cyber-crime* (or "Budapest Convention"). It is the only binding international instrument dealing with cyber-crime and it was opened to signatures in 2001, entering into force in 2004. Canada, Japan, South Africa and the US participated in its elaboration and signed the final document, although only the US had actually had it ratified. The Convention is not limited to members of the Council of Europe. But it has not been widely endorsed by Latin American countries. Whilst open to non-European states, not one Latin American country has acceded to the Protocol. Although a few Latin American and Caribbean countries have been invited to join the Convention[25], none has been able to meet the necessary requirements to accede.[26] Many also object to the perceived Euro-centric nature of the Convention´s drafting and content.[27] Indeed, Latin American countries are largely absent from wider strategic international debates on cyberspace.[28]

"Most countries in Latin America have developed strategies to deal with cyber-crime in line with the OAS´s Comprehensive Strategy"

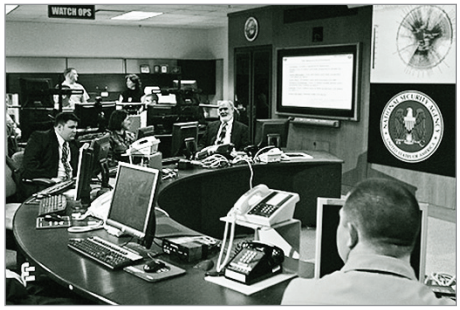
25 Countries such as Argentina, Chile, Cost Rica, Dominican Republic and Mexico have been invited.

26 The requirements for entry include the existence of a specific legal framework covering all categories of cyber-crime, solid procedural legislation, an advanced state of international cooperation, and the existence of a CSIRT.

27 European expertise, standards and good practices on the matter are often used as guidelines for governments and organizations in the region to design and implement policies.

28 According to Camino Kavanagh, with the exception of Brazil, Latin American countries are not actively involved in discussions on internet freedom, internet governance or wider UN debates. For its part, Brazil is largely working on related issues through the India-Brazil-South Africa forum. Interview, May 2012.

Although there are no binding international treaties on cyber-crime from the UN, some agencies are pushing ahead to better define intervention points. The two key agencies in this regard are the UN Office on Drugs and Crime (UNODC) and the ITU. For its part, the UNODC is concerned with the ways in which organized crime organizations, drug trafficking entities, piracy groups and money-laundering syndicates are mobilizing new technologies to advance their aims. It established an open-ended intergovernmental expert group in 2010 to undertake comprehensive studies on the issue with a view of identifying legal and operational responses.[29] Notwithstanding meetings in 2011 and 2012, the study has yet to materialize. Meanwhile, the ITU initiated activities in 2003 and in 2006 declared cyber-security as one the agency´s top three priorities. In 2007 it launched the Global Cyber-Security Agenda and convened a high-level group of more than 100 experts.[30]



"There is comparatively little evidence of bilateral cooperation between Latin America countries on managing cyber-security and cyber-defence"

Meanwhile, most countries in Latin America have themselves developed strategies to deal with cyber-crime in line with the OAS´s Comprehensive *Inter-American Strategy to Combat Threats to Cyber-security*. Adopted by the OAS General Assembly in 2004, the strategy is overseen by the Committee on Hemispheric Security and three departments that manage implementation: (i) the Inter-American Committee Against Terrorism (CICTE); (ii) the Inter-American Telecommunication Commission (CITEL); and (iii) the Group of Governmental Experts on Cyber-Crime from the Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA).[31] In addition to providing technical assistance, these entities draw attention to key issues through conferences, seminars and exchanges, as well as support for establishing computer security incident response teams, or CSIRTs.[32]

A number of other multilateral mechanisms exist that are also supporting cyber-crime capabilities and response across Latin America. For example, some Latin American countries are receiving assistance through the Economic Commission for Latin America and the Caribbean (ECLAC). Key modalities of support from ECLAC include technical assistance and information provided by the Observatory for the Information Society in Latin America and the Caribbean (OSILAC), established in 2003. Likewise, the recently formed Union of South American Nations (UNASUR) has also held meetings between the Defence, Justice and Interior Ministers of the twelve countries that ratified the founding treaty in order to

29 Paragraph 42 of the 2010 Salvador Declaration notes: "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime.

30 See ITU website at: http://www.itu.int/osg/csd/cyber-security/gca/hleg/members.html (accessed March 15, 2012).

31 Interview with Adam Blackwell, Secretary for OAS Multidimensional Security, in April 2012.

32 The CSIRT concept emerged in 1988 following the Morris worm incident, with the creation of the so-called coordination center at the software engineering institute (CERT), a US FFRDC operated by Carnegie Mellon University. The model was soon replicated in the US and abroad.

review cyber-defence capabilities.[33] Meanwhile, the Andean Community has also drawn attention to the issue since 2004, when it established a common external security policy. The policy includes provisions for more cooperation and coordination of national actions.[34] Other mechanisms such as the Network of E-government Leaders of Latin America and the Caribbean (RedGEALC)[35] and the Latin American Forum of Telecommunications Regulators (Regulatel), including 20 government regulators,[36] are also involved in aspects of information security and cyber-crime.

There is comparatively less publicly available evidence of bilateral cooperation between Latin America countries on managing cyber-security and cyber-defense. While this is a possible area of growth, just one country has signed a treaty – Brazil – with another country outside of Latin America – Russia. The *Agreement on Non-Aggression by Information Weapons* was signed in 2010 and represents the first bilateral agreement of its kind. In addition to a pact of non-aggression in the case of a conventional war, the agreement calls for information exchange, capacity strengthening and joint cyber-war exercises. Meanwhile, the Defense Ministers of Argentina and Brazil also signed a 2011 *Joint Declaration* to review bilateral cooperation across the defence sector, with one clause specifically calling for increased cooperation on informatics and cyber-defence. Likewise, Likewise, Defence Ministers from Brazil, Chile and Colombia have also expressed their concerns to the US Pentagon regarding cyber threats such as hacktivism and have urged for the hardening of computer networks against breaches and increased cooperation.[37]

Operational responses at the national level

Given the heterogeneity of the cyber-security threat, Latin American countries are adopting similarly diverse responses to establish safer and more secure cyberspace. While drawing some inspiration from the above-mentioned international and regional conventions, most national responses are in fact shaped by practical considerations associated with local ICT infrastructure and economic interests. Even so, there are some common features to national government responses. Key activities include the development of *specific legislation on cyber-crime*; the creation of *specialized police units or other specialized law enforcement agencies*; *the formation of a national CSIRT*; and *the constitution of executive branch specialized units*. And whilst there are other efforts being pursued,[38] these are widely considered the most important.

33 Approaches to containing transnational organized crime were reviewed in February 2012, and the Defense Strategic Studies Center (CEED) established in 2011 will likely deepen its engagement on the issue.

34 See Colombian Government (2011) *Lineamientos de Política para Ciberseguridad y Ciberdefensa*. Bogotá: DNP/CONPES.

35 See http://www.redgealc.net (accessed March, 05, 2012).

36 The list with the members of the organization is available at: http://www.regulatel.org/j/index.php?option=com_content&view=article&id=114&Itemid=79 (accessed March 11, 2012). Regulatel also counts with three European observer agencies from Portugal, Spain and Italy.

37 See Baldor, L. (2012) "US Sees South America as Possible China Counter". *Associated Press*, April, 28. Available at: http://news.yahoo.com/us-sees-south-america-possible-china-counter-140345250.html.

38 For example, there are technical commissions (e.g. Dominican Republic's *Comisión Interinstitucional Contra los Crimenes y Delitos de Alta Tecnología*); national observatories (e.g. Argentina's Social Networks Observatory against Cyberbullying); certificate authorities (e.g. Uruguay's PKI, Public Key Infrastructure); and national strategies, plans and conferences (e.g. Colombia's "Lineamientos de Políticas para Ciberseguridad y Ciberdefensa" from 2011).

A growing number of Latin American countries have elaborated specific **legislation** on cyber-crime.[39] Indeed, the OAS has sought to ensure that some of the key provisions of the Inter-American Strategy are aligned with existing national legislation.[40] And while definitions of cyber-crime vary between countries, there are several categories on which most states agree that penalization can occur – electronic transactions, electronic signature and authentication, consumer protection, data protection, cyber-crime prosecution, intellectual property, domain names and taxes and customs.[41] Using these criteria, there are at least six Latin American countries reviewed in the preparation of this **Strategic Paper** that have yet to develop clear and specific laws to penalize cyber-crimes – Belize, Brazil, Cuba, El Salvador, Honduras and Nicaragua. Meanwhile, Guyana and Suriname only have limited references in their penal codes for offences that could constitute cyber-crime (see Figure 2).

"The tensions between individual privacy and the demands of law enforcement are obvious"

In spite of these efforts to shore up such legal and operational responses, there are some concerns about the ways in which certain governments across Latin America are bolstering their surveillance of cyberspace. For example, content filtering of the internet is increasing dramatically in some countries. As observed by the group OpenNet Initiative, the protection of children is often invoked as a pretext to filter internet content in Latin America.[42] Nevertheless, child pornography and pedophilia remain concerns across the region, as elsewhere, with a growing number of governments and non-governmental agencies taking up the cause. For example, the NGO Safernet Brazil has highlighted how the lack of monitoring of website traffic by Latin American law enforcement sites has resulted in their proliferation, including in havens such as Panama.[43] The tensions between individual privacy and the demands of law enforcement are obvious.

39 According to the OAS, the most comprehensive legislation is the Dominican Republic's 2007 Ley No. 53-07 sobre Crimenes y Delitos de Alta Tecnologia.

40 See http://www.oas.org/juridico/english/cyber_legis.htm (accessed May 08, 2012).

41 See UNCTAD (2009) *Estudio Sobre las Perspectivas de la Armonización de la Ciberlegislación en América Latina*. New York: UNCTAD/DTL/STICT, June, 56.

42 See OpenNet Initiative, http://opennet.net/research/regions/la (accessed April 21, 2012).

43 According to SaferNet, "child pornography websites are sprouting up more frequently in Latin America […] and many of these sites were hosted in the Czech Republic, but with [pressure from authorities], they started becoming available in countries like Panama, where 100 new [child] pornography domains have already been registered". http://infosurhoy.com/cocoon/saii/xhtml/en_GB/features/saii/features/main/2011/10/03/feature-01 (accessed April 21, 2012).

Figure 2. Key legislation for cyber-crime in selected Latin American countries (2012)[44]

Country	Name and/or reference of the legislation
Argentina	Ley 26.388 de Delitos Informáticos (2008)
Bolivia	Ley 1768 de Delitos Informáticos (1997)
Chile	Ley 19.223 de Delitos Informáticos (1993)
Colombia	Ley1273 de la Protección de la Información y de los Datos (2009) + Ley 527 de Mensajes de datos, del Comercio electrónico y de las Firmas digitales (1999)
Costa Rica	Ley 8148 de Delitos Informáticos (2001)
Dominican Republic	Ley 53 de Delitos Informáticos (2007)
Ecuador	Ley 67 de Comercio electrónico, Firmas y Mensajes de datos (2002)
Guatemala	Penal Code altered to include cyber-crime (2000)
Mexico	Penal Code altered to include, among others, cyber-crime (1999)
Panama	Articles 216, 222, 283, 284, 362 and 364 of the Penal Code + Art. 61 from Ley 51 (2008): Documentos y Firmas Electrónica
Paraguay	Ley 1.160 (1997) alters the Penal Code in order to include, among other things, cyber-crime
Peru	Ley 27.309 de Delitos Informáticos (2000)
Uruguay	Ley 17.616 de Protección del Derecho de Autor y Derechos Conexos (2003): contains explicit provisions regarding digital intelectual property
Venezuela	Decreto 48 (2001): Ley Especial Contra los Delitos Informáticos

Meanwhile, there is growing investment in enhancing **law enforcement capacities** to address cyber-crime. Specialized units have been established with the necessary capacities and tools, including investigative capacities (see Figure 3).[45] Such units are not necessarily devoted exclusively to monitoring internet-based crime, but also work on crimes supported by virtual means. For example, the Mexican cyber-police, the first of its kind in Latin America, works closely with local NGOs to deal with all manner of crimes, from narco-trafficking to child prostitution networks. The Chilean Investigative Brigade on Cyber-crimes (BRIBIC) also works on a combination of financial crimes, computer

44 See REMJA website and ECLAC, *Panorama del Derecho Informático en América Latina y el Caribe* and other sources.

45 Although Ecuador, Panama, Paraguay and Venezuela do not appear in the list above, these countries feature institutions that serve as specialized police forces on cybercrime.

forensic analysis, and child pornography. Alongside the Brazilian Cybercrime Repression Unit (URCC) managed by the federal police is an array of state-level police stations that are specialised in cybercrime.[46] These and other groups often work with Interpol on the Latin American Working Group of Experts on Information Technology Crime.

Figure 3. A sample of police units devoted to cyber-crime in Latin America (2012)

Country	Name of the Unit
Argentina	*División de Seguridad Informática Federal* de la Superintendencia del Interior – Policía Federal Argentina (PFA)
Bolivia	*División Delitos Informáticos* de la Fuerza Especial de Lucha contra el Crimen (FELCC) de la Policía Nacional
Brazil	*Unidade de Repressão a Crimes Cibernéticos* (URCC) da Polícia Federal
Chile	*Brigada Investigadora de Ciber Crimen* (BRICIB) de la Jefatura Nacional de Delitos Económicos – Policía de Investigaciones de Chile (PDI)
Colombia	*Grupo de Investigaciones Tecnológicas* de la Subdirección de Investigación Criminal (Área Investigativa contra el Patrimonio Económico) de la Dirección de Investigación Criminal e Interpol (DIJIN) de la Policía Nacional de Colombia
Dominican Republic	*Departamento de Investigación de Crímenes de Alta Tecnología* (DICAT) de la Dirección Central de Investigaciones Criminales (DICRIM) de la Policía Nacional
Honduras	*Unidad Especial de Delitos Informáticos* de la Dirección Nacional de Servicios Especiales de Investigación de la Policía Nacional
Mexico	*Policía Cibernética* del Sector de Inteligencia de la Policía Federal Preventiva (PFP) y de la Subsecretaría de Tecnologías de la Información de la Secretaría de Seguridad Pública Federal (SSP)
Peru	*División de Investigación de Delitos de Alta Tecnología* (DIVINDAT) de la Dirección de Investigación Criminal y de Apoyo a la Justicia (DIRINCRI) de la Policía Nacional
Uruguay	*Departamento de Delitos Informáticos* de la Policía Nacional

Arguably the most important institutions involved in addressing cyber-crime are **CSIRTs**. Such units have been created across Latin America, with most governments devoting considerable resources to getting them off the ground (see Figure 4). Likewise, the OAS has supported governments across the region, including in partnership with the Coordination

46 There are a number of specialized law enforcement agencies in the four countries that are not clearly linked with the national police forces. These include the Paraguayan *Unidad Especializada de Delitos Informáticos de la Fiscalia General del Estado*, the Panamanian *Fiscalía Especializada en Delitos contra Propiedad Intelectual y Seguridad Informática*, the Ecuadorian *Unidad de Delitos Informáticos del Ministerio Público* (UDIMP), and the Venezuelan *División contra Delitos Informáticos del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas* (CICPC) of the Ministry for Internal Relations and Justice (*Ministerio del Poder Popular para Relaciones Interiores y Justicia*). These agencies are mandated to revent, investigate, and prosecute all cyber-crime activities. In the cases of Paraguay, Panama and Ecuador, they are connected to the public prosecutors office.

Center at Carnegie Mellon University, or CERT/CC. While often serving as a focal point for national efforts to contain cyber-crime, CSIRTs are hardly uniform. For example, in Colombia, the so-called colCERT has a broad mandate ranging from strengthening ministerial capacities (Justice and Interior), adopting global standards (Foreign Affairs), developing cyber-security and cyber-defense measures (Defence).

Figure 4. A sample of CSIRTs across Latin America (2012)

Country	CSIRTs
Argentina	ArCERT (Coordinación de Emergencias em Redes Teleinformáticas de la República Argentina)
Brazil	CERT.Br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)
	CTIR Gov (Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal)
Chile	CLCERT (Chilean Computer Emergency Response Team)
	CSIRT – GOB
Colombia	colCERT (Centro de Respuesta a Emergencias Cibernéticas de Colombia)
Guatemala	CSIRT.Gt (Centro de respuestas a incidentes de seguridad informática de Guatemala)
Mexico	UNAM – CERT (Equipo de Respuesta a Incidentes de Seguridad en Cómputo de la Universidad Nacional Autónoma de México)*
Paraguay	CSIRTPy (Equipo de Respuesta a Incidentes de Seguridad de Paraguay)
Peru	peCERT
Uruguay	CERTUy (Centro Nacional de Respuesta a Incidentes en Seguridad Informática)
Venezuela	VenCERT (Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela)

** The Mexican CSIRT is located in a university and addresses incidents nationally.*

Finally, some specialized executive units have been developed by national governments in Latin America to address cyber-crime and protect digital information. Many of these owe their existence to the increased reliance of governments on e-services and e-governance (see Figure 5). As noted by Mandarino and Canongia, it is necessary for public administrations "to guarantee the availability, integrity, confidentiality and authenticity of digital information in order to formulate strategies and decision-making," including through the protection of both governmental and societal cyberspaces.[47]

47 See Canongia, C. and Mandarino Junior, R. (2009) "Segurança Cibernética: o desafio da nova Sociedade da Informação." *Parceria Estratégica*, Vol. 14, no. 29 (jul-dec): 23.

Most of these units tend to be attached directly to the executive branch, including the president´s office or a specific ministry. For example, in Peru the so-called ONGEI prioritizes information security and has promoted cyber-security across departments.

Figure 5. **Figure 5. A sample of executive branch specialized units (2012)**

Country	Specialized Unit
Argentina	ONTI - *Oficina Nacional de Tecnologías de Información* de la Subsecretaría de Tecnologías de Gestión (SsTG) de la Jefatura de Gabinete de Ministros de la Presidencia de la Nación
Brazil	DSIC – *Departamento de Segurança da Informação e Comunicações* do Gabinete de Segurança Institucional da Presidência da República (GSI)
Dominican Republic	OPTIC - *Oficina Presidencial de Tecnologías de la Información y Comunicación*
Mexico	IFAI – *Instituto Federal de Acceso a la Información y Protección de Datos*
Peru	ONGEI – *Oficina Nacional de Gobierno Electrónico e Informática* de la Presidencia del Consejo de Ministros (PCM)
Uruguay	AGESIC – *Agencia de Gobierno Electrónico y Sociedad de la Información*
	URCDP – *Unidad Reguladora y de Control de Datos Personales*
Venezuela	CNTI – *Centro Nacional de Tecnologías de Información*

There is comparatively limited information on the extent to which militaries and intelligence services are involved in cyber-security and cyber- war activities. Notwithstanding the considerable investments in North American, Western European and some Asian militaries in cyber-security and cyber-defence efforts[48], this does not seem to be the case in Latin America. The issue is still comparatively new, and governments are still playing catch-up in many respects. Moreover, with the exception of Colombia, terrorism and warfare are not as clear and present a threat as in many other regions. Another exception appears to be the *Centro de Defesa Cibernética do Exército Brasileiro*, or CDCiber (Cyber-defence Center of the Brazilian Army).[49] It was funded in 2010 and became operational the same year.[50] CDCiber was designed to coordinate the cyberdefence actions of the army, and eventually with the navy and air-force with the principal task of protecting governmental and military networks from external and internal attacks.[51] According to the Brazilian

48 See for example the efforts of the US Cyber Command (USCYBERCOM) of the armed forces and the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), based in Tallinn, Estonia.

49 This does not exclude the possibility that other governments in the region have initiated military programs. Colombia, for example, has plans to establish a new center. The Dominican Republic Armed Forces, participating in the CICDAT, are also increasingly involved in cyber-security related issues.

50 The creation of CDCiber reflected Brazil's 2008 National Defense Strategy (END) and its central focus on cybernetics together with space and nuclear technologies.

51 CDCiber houses a cyber-warfare simulator, a laboratory to analyze malicious software, and at least 100 officers trained in cyber-security.

Commander of CDCiber, its first test will be the Rio+20 Conference in June 2012 while its second and third include the World Cup in 2014 and Olympics in 2016.[52] As for intelligence services, there were just two examples generated in the course of this research, from the Dominican Republic[53] and Brazil.[54]

Private sector and civil society responses

While there is growing appreciation of the dimensions of cyber-crime in countries such as Brazil, Colombia, Mexico, and across Central America, there is less intellectual engagement on the topic from public and private universities or independent research institutes than might be expected (see Annex 2). Rather, research on issues of cyber-security is shaped to a large extent by market forces, with businesses investing in cyberlaw and computer sciences. A growing number of private companies and consultancy firms appear to be heavily investing in capacities across both areas. As a result, there is an absence of any serious comprehensive or inter-disciplinary investigation related to the causes and wider consequences of cyber-crime and cyber-security, and much less analysis available that could be applied to the development

"A growing number of civil society organizations are supporting services and awareness-raising in relation to cyber-security in Latin America"

of more effective public policies. This is a market failure that concerned governments would do well to fill.

One important exception at the regional level is the non-governmental organization *Latin American Cooperation of Advanced Networks* (RedCLARA), which seeks to connect institutions working on the issue of cyber security. Specifically, RedCLARA connects 15 Latin American academic networks, such as Brazil's RNP (*Rede Nacional de Pesquisa e Ensino*) and Peru's RAAP (*Red Académica Peruana*). With support from the European Commission, the association serves as "a Latin American collaboration system by means of telecommunications, advanced networks for research, innovation and education." One particular effort of RedCLARA is the hosting of the TICAL Conferences (*Tecnologías de la Informácion y Comunicaciones en América Latina*) – organized by the heads of the computer science departments of participating institutions – which virtually always include sessions on cyber-security and undertake outreach with CSIRTs.

52 See http://www1.folha.uol.com.br/tec/1085498-rio20-e-teste-para-novo-centro-de-defesa-cibernetica-leia-entrevista-com-general.shtml.

53 For example, the Dominican Republic´s intelligence agency (J-2 of the Ministry of Armed Forces) provides essential support and relevant information to DICAT, the national cyber-crime specialized police unit.

54 In Brazil, the *Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações* (CEPESC, Research and Development Center for Communications Security) from ABIN, the Brazilian central intelligence agency, is actively involved in protecting the federal public administration's cyberspace, namely through cryptographic activities.

By way of contrast, a growing number of civil society organizations are supporting the development of services and awareness-raising functions in relation to cyber-security in Latin America. Owing in large part to the dispersed and de-centralized nature of cyberspace, non-governmental institutions are in fact well positioned to expand their activities in this regard. Many are already deeply invested in shaping the internet architecture through, for example, the attribution of domain names – a key element for preserving network stability and security. This is the case, for instance, of the *Latin American and Caribbean Network Information Centre* (or LACNIC).[55] The LACNIC is intended to allocate and administer IP addresses across the region and is one of five regional registries around the world. In 2009, LACNIC launched the *Amparo Project* with the objective of strengthening regional capacities to handle computer security incidents. Another key actor is the International Information Systems Security Certification Consortium (ISC²) which is a not-for-profit entity to support training and standards. It includes a network of more than 75,000 industry experts, including in Latin America. Finally, the Information Systems Security Association (ISSA) has supported initiatives in Latin America, including the first "Latin American Cyber-defence" conference in April 2012.

There has been a marked growth in associations and digital communities that are substituting for the lack of engagement by government, research institutions and the private sector in cyber security. Prominent examples in Latin America include the *Asociación Latinoamericana de Profesionales en Seguridad Informática* (ALAPSI) and the Brazilian *Associação Brasileira de Especialistas em Alta Tecnologia* (ABEAT). Additional groups such as the *Federación Iberoamericana de*

"Private corporations play a marginal role in supporting cyber-security initiatives and enhancing public safety in cyber-space"

Derecho e Informática (FIADI, Law and Informatics Ibero-American Federation)[56] and *CXO LatAm Community*, a Latin American community of IT and information security managers. Even more prominent than some of these groups are web-based NGOs and individual experts working on cyber-crime issues that are contributing to the field, notably through making available up-to-date content and news.[57] Examples of web-based NGOs include *Ciberdelincuencia.org*, formed by a Mexican expert, and Argentina's *Cibersegura*, owned by an Argentinian specialist. Other NGOs, such as *Algo Tenemos que Hacer* in Argentina and *Derechos Digateles*, based in Chile, are increasingly prominent in monitoring cyber-crime and related offences and offering information.

55 The LACNIC serves in some ways as the regional representative of the Internet Corporation for Assigned Names and Numbers – or ICANN. The ICANN provides global coordination of the Internet Domain Name System (DSN) and also sets standards and policies to ensure constant security and stability across the worldwide web.

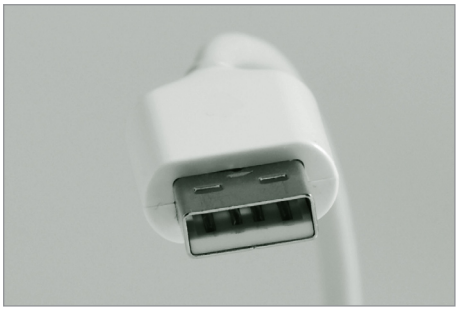
56 FIADI congregates people and institutions particularly interested in cyberlaw, including those from Portugal and Spain. In addition to the magazine "Revista Iberoamericana de Informática y Derecho", FIADI also organizes the annual congress "Congreso Iberoamerican de Derecho e Informática".

57 Examples of individual initiatives are: Crimes Cibernéticos, Hacking Mexico, Soy Forense, Derecho Informático, and ICT Pulse.

Although not a key focus of this study, the private sector obviously has a particular stake in cyber-security. And yet, in Latin America, private corporations and firms appear to be playing a comparatively marginal role in supporting cyber-security initiatives and enhancing public safety in cyber-space. Not a single public-private partnership could be identified in the course of the preparation of this **Strategic Paper** in Latin America. Of course some private firms have a particular interest in shedding light on the issue – not least McAfee, Kaspersky Labs and Symantec to name a few – but they are more the exception than the rule. What is obvious is that major hardware and software firms, banks and e-commerce companies are clearly undertaking focused efforts to ensure that electronic transactions are secure for their clients and personnel. However, their efforts seem to end there. Most are reluctant to share information on the scale of their losses to federal or district level authorities. As noted in the *Security and Defense Agenda's* report: "[t]he problem is that companies are reluctant to talk about these (cyber-crime issues); they aren't keen to reveal vulnerabilities to competition or to consumers, and they also have data privacy rules to contend with."[58]

In Latin America, as elsewhere, the banking sector is the most preoccupied with the threat of cyber-crime. Many have introduced safety measures, including new password-protection and code schemes. Some associations of Brazilian, Dominican Republic, Honduran and Mexican banks – respectively, *Federação Brasileira de Bancos* (FEBRABAN), *Comisión Nacional Bancaria y de Valores*, *Superintendencia de Bancos and Comisión Nacional de Bancos y Seguros* – have taken important concerted measures with governmental bodies, especially central banks, in order to provide a safer

"Latin American countries have so far managed to avoid the militarization of their cyberspace"



cyber-space for their members.[59] But few, if any, cooperate outside of their sector. In the meantime, ICT companies and some smaller technology firms are more predisposed to collaboration, primarily through the organization of seminars on the topic. Some also maintain digital platforms featuring up-to-date information on cyber-security.[60] A regional mechanism, called eCom-LAC, has emerged to facilitate such collaboration across the private and public sectors in order to establish more secure internet environments and guarantee the integrity of the millions of e-commerce digital transactions occurring daily.[61]

58 See Security and Defense Agenda (2011), 35.

59 As an example of cooperation, the Brazilian FEBRABAN and Federal Police established an agreement on cyber-security issues aiming the 2014 World Cup in the country (website accessed on March 30, 2012). Source: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=28140&sid=18

60 Examples include *Segu-Info, AntiFraude, Informática Legal, Identidad Robada, CybSec and Lex Informática*. Most of them are based in Argentina.

61 This is called the *Federación Latinoamericana y Caribe de Internet y el Comercio Electrónico* (eCOM-LAC, Latin American and Caribbean Federation for Internet and e-Commerce) which has permanent partnerships with ICANN, LACNIC and ISOC.

Meanwhile, there is some evidence that a small number of private actors are beginning to assume a greater role in cyber-security. For example, chambers of commerce, intellectual property organizations and film and music producer associations are asserting themselves. Campaigns to fight digital piracy are spreading.[62] Perhaps one of the most obvious ways that private groups are engaging is through the organization of open and closed seminars on cyber-security. For example, both Kapersky Laps and Microsoft have assigned specialists across the region to participate in events. Likewise, the US-based TeleStrategies is to hold a major cyber-security event in Brasilia in July 2012 targeting Latin American specialists. A central topic of the event relates to fighting drug trafficking, cyber money-laundering, human trafficking, terrorism and other criminal activities conducted over telecommunications networks and across the internet. Despite these efforts, it should be stressed that a major assessment of the overall engagement of the private sector on issues of cyber-security in Latin America found that its standards and participation were "marginal to poor" when compared to those of other regions.[63]

Concluding reflections and future research

Cyber-security is emerging as a dominant area of concern amongst many governments and civil societies across Latin America. Latin America´s response to cyber-crime is more or less in line with the perceived threats generated by organized crime, single users, and smaller-scale political activism. Latin American governments and societies are less preoccupied with threats of cyber-war or cyber-terrorism or with issues of rights to digital privacy and freedom – at least not yet. With few exceptions, Latin American countries have so far managed to avoid the militarization of their cyberspace, which would include, for example, a more active role of national militaries.

At the same time, responses to cyber-crime are comparatively underdeveloped in Latin America and are highly concentrated in just a small selection of countries. While some governments have initiated more robust and comprehensive responses, most are only at the beginning stages of mounting an effective strategy. Indeed, both public and private responses to cyber threats in selected Latin American countries are rated as poor according to governmental and industry standards set by groups such as PriceWaterhouseCoopers and the Security and Defense Agenda.[64] A recurring challenge is the narrow construction of the cyber threat as one of new criminality only and the dominance of legal and computer sciences when it comes to formulating responses. With many governments and civil societies just beginning to articulate responses to cyber-crime, the region has become a potential safe haven for cyber-crime. There continue to be marked regional disparities and capacity gaps, and these could be usefully addressed by more collaboration and coordination amongst governments in the region.

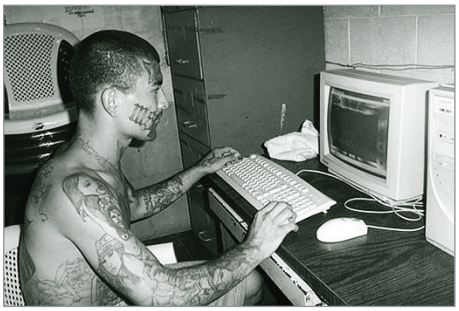
62 The Brazilian *Associação Antipirataria de Cinema e Música* (APCM, Music and Film Anti-piracy Association), for instance, is an association that was created precisely for this end.

63 See PricewaterhouseCoopers (2011) *Pesquisa Global de Segurança da Informação 2012*. São Paulo: PricewaterhouceCoopers.

64 In its assessment, SDA considers the following indicators : 1) applying basic rules of cyber hygiene; 2) using computer network defense (CND) tools, like anti-virus, firewalls, intrusion detection/protection, and strong identity management (such as electronic signatures); 3) exchanging standards and data to create a robust and interoperable cyber ecosystem; 4) adopting a more agile defence posture, with innovative cyber-defences tapping into advanced sensors and intrusion prevention systems from the host to the gateways; and 5) consolidating a predictive cyber-readiness and agility within its domains and with partners. See Security and Defense Agenda (2011), 50.

The scale of cyber-crime in Latin America is likely to get worse before it gets any better. Future research will need to move beyond reporting on the manifestations of new crime to grappling with the actors and underlying conditions shaping the rise of cyber-criminality. The existence of cyberspace is already generating a massive evolution – indeed a revolution – in all aspects of social, economic and political life. It is by definition extending the reach of organized crime across time and space. And given Latin America´s youthful demographics, future research will need to consider the underlying conditions shaping the mobilization of cyber-criminals. At one end are narcotics syndicates that mobilize through cyberspace to intimidate, harass and challenge state and civil society groups. At the other end are emerging social-protest movements that are already transcending borders, with implications for elections and governance.[65]

"Latin American governments must devote greater attention to defining norms to govern cyberspace and ensure they take balanced measures"



It is urgent that Latin American governments devote greater attention to defining norms to govern cyberspace and ensure they take balanced measures. On the one hand, governments must begin adopting more sophisticated approaches to regulating content as a means of addressing some of the perverse outcomes of cyber-crime. Likewise, private sector entities should also be encouraged to adopt more proactive actions since they have much to lose from intellectual property theft, piracy and a range of criminal offences. Meanwhile, civil society groups should be supported to draw attention to the implications of such measures on the state-citizen relationship and in particular, privacy.[66] There is a danger that government responses err too far towards a securitized response, emphasizing surveillance and repression. While a delicate balancing act, efforts to fight cyber-crime must be carefully attuned to the fundamental rights of citizens.

65 See, for example, http://www.miradorelectoralguatemala.org/ushahidi-new/.

66 See, for example, Deibert, R. and Rohozinski, R. (2010) "Risking Security: Policies and Paradoxes of Cyberspace Security", International Political Sociology 14 (1).

Annex 1. Internet access across Latin America (2012)

Sub-region	Country	Internet Users	Percentage of the Population (%)
Central America	Belize	63,580	19.8
	Costa Rica	2,000,000	43.7
	El Salvador	1,257,380	20.7
	Guatemala	2,280,000	16.5
	Honduras	1,067,560	13.1
	Mexico	42,000,000	36.9
	Nicaragua	663,500	11.7
	Panama	1,503,441	43.4
Caribbean	Antigua and Barbuda	70,968	80.8
	Bahamas	158,700	50.7
	Barbados	191,878	66.9
	Cuba	1,702,206	15.4
	Dominican Republic	4,120,801	41.4
	Haiti	836,435	08.6
	Jamaica	1,581,100	55.1
	Puerto Rico	1,698,301	42.6
	Trinidad and Tobago	650,611	53.2
South America	Argentina	28,000,000	67.0
	Bolivia	1,985,970	19.6
	Brazil	79,245,740	39.0
	Chile	10,000,000	59.2
	Colombia	25,000,000	55.9
	Ecuador	4,075,500	27.2
	Guyana	225,593	30.3
	Paraguay	1,523,273	23.6
	Peru	9,973,244	34.1
	Suriname	165,733	33.7
	Uruguay	1,855,000	56.1
	Venezuela	10,976,342	39.7

Internet World Stats, http://www.internetworldstats.com (accessed April 19, 2012)

Annex 2. A sample of Latin American research institutes involved in cyber security (2012)

Institution	State	Description
UCA – Universidad Católica Argentina	ARG	It has a specialization in high technology law, having trained many of the Argentinean cyber law experts. UCA has already organized conferences on the subject
EST – Escuela Superior Técnica del Ejército	ARG	It trains computer engineers specialized in Information Security for the Armed Forces, who are also able to deal with cryptography
Cyber Forensic Training Center	BAR	One of the few places in the Caribbean which can provide training in cyber forensics. It is an initiative from the US Embassy to the country, which had established a Regional Cyber Investigations Laboratory (RCIL) in Antigua in 2009
NUPRI – Núcleo de Pesquisa de Relações Internacionais (USP)	BRA	NUPRI from University of São Paulo has researchers carrying out studies on broader questions of cyber-security, such as a comparative study of Latin American countries' cyber-security strategies
CEGSIC – Curso de Especialização em Gestão da Segurança da Informação e Comunicações (CIC-UnB)	BRA	CEGSIC is training most of the Brazilian public administration experts on cyber-security. They are at present preparing a thorough study on how Brazil federal governmental structures are protecting their cyberspace
UFABC – Universidade Federal do ABC	BRA	The Research Center on Science, Technology and Society is very active in analyzing the causes and consequences of hacktivist movements
Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile	CHI	One of the few research centers on cyberlaw in LAC region, it also publishes the journal "Revista Chilena de Derecho Informático"
ITLA – Instituto Tecnológico de Las Américas	DOM	Besides being a constitutive member of the governmental commission CICDAT (Comisión Interinstitucional Contra los Crimenes y Delitos de Alta Tecnología), it also organizes regional conferences on cyber-security, such as the "Reunión de Actores Nacionales en materia de Seguridad Cibernética"
FUNGLODE – Fundación Global Democracia y Desarrollo	DOM	The Security and Defense Research Center of FUNGLODE recently started up an initiative on the state of cyber-security in the continent
ITESM - Instituto Tecnológico y de Estudios Superiores de Monterrey	MEX	One of the most respected Mexican institutions in technological training, ITESM has one of the few centers in Central America focused on research and innovations in computer security
Laboratorio de Seguridad Informática de UNAM - Universidad Autónoma de México	MEX	Apart from offering courses on information security it also has a research group on cyberlaw. UNAM has already organized many conferences such as the "Congresso Seguridad en Cómputo" in 2011. UNAM manages the Mexican national CSIRT
Centro de Investigación, Desarrollo e Innovación en TICs de la Universidad Tecnológica de Panamá	PAN	It is also one of the few research centers carrying out research and developing new ICT tools in Central America, including cyber-security components
Universidad Católica de Táchira, Facultad de Ciencias Jurídicas y Políticas	VEN	Representing one of the rare long-term research groups on cyber law in LAC countries, it also publishes the journal "Derecho y Tecnología: Revista arbitrada de Derecho y Nuevas Tecnologías"

IGARAPÉ INSTITUTE is a southern think tank devoted to evidence-based policy and action on today and tomorrow's complex challenges. The goal of the Institute is to stimulate evidence-based and humane engagement on present and emerging security and development issues.

INSTITUTO IGARAPÉ é um think-tank dedicado à integração das agendas de segurança e de desenvolvimento. Seu objetivo é propor soluções alternativas a desafios sociais complexos, através de pesquisas, formulação de políticas públicas e articulação.

THE SECDEV FOUNDATION is a not-for-profit organization that seeks to broaden global public awareness and understanding in three core programme areas: cyber-empowerment; the sources of security and resilience; and, armed violence prevention and reduction. The SecDev Foundation supports local partners, research and advocacy in regions at risk from fragility, violence and underdevelopment in Asia, Africa, Eurasia, the Middle East and Latin America.

THE STRATEGIC PAPER series is published by the Instituto Igarapé.

Designer
Kenia Ribeiro

Address
Visconde de Caravelas 111
Botafogo. Rio de Janeiro – RJ
22271-030 Brasil

Rio de Janeiro: +55 21 3283-7073
Brasília: +55 61 3526-1960
E-mail: contato@igarape.org.br
Site: www.igarape.org.br

OTHER PUBLICATIONS BY THE IGARAPE INSTITUTE

STRATEGIC BRIEF 1 – MARCH 2012

HAITI´S URBAN CRIME WAVE? RESULTS FROM MONTHLY HOUSEHOLD SURVEYS (AUGUST 2011-FEBRUARY 2012)

POST-EVENT REPORT 1 – APRIL 2012

EXPANDING THE CIVILIAN ROLE IN PEACE OPERATIONS: ASSESSING PROGRESS AND ADDRESSING GAPS

STRATEGIC PAPER 1 – MAY 2012

MECANISMOS NACIONAIS DE RECRUTAMENTO, PREPARO E EMPREGO DE ESPECIALISTAS CIVIS EM MISSOES INTERNACIONAIS

INSTITUTO IGARAPÉ

TheSecDev foundation

IDRC | CRDI Canada