CYBERSECURITY IN LATIN AMERICA AND THE CARIBBEAN:

the state of readiness for the defense of cyberspace

Dr. Boris Saavedra

William J. Perry
Center for Hemispheric Defense Studies

July 2015

Book cover by
Viviana Edwards

CYBERSECURITY IN LATIN AMERICA AND THE CARIBBEAN:
the state of readiness for the defense of cyberspace

It has become appallingly obvious that our technology has exceeded our humanity.
Albert Einstein

The best minds are not in government. If any were, business would steal them away.
Ronald Reagan

Information and Communication Technology (ICT) is the driving force behind the evolution of modern societies and cybersecurity is paramount for sustaining a technologically-sound model. The disruption of electricity or the impairment of financial systems through interference with ICT networks is a reality; these events constitute national security threats. Malicious online agents are numerous, organized and of diverse origins: political, criminal, terrorist, hacktivist. Therefore, computer security is developed with three main objectives: availability, confidentiality and integrity. The best way to categorize an attack is by assessing the vulnerability of these objectives to a threat.

The objective of this paper is to analyze the readiness capabilities of Latin America as a region and its ability to confront cyber threats according to the *Global Cybersecurity Index & Cyberwellness Profiles* April 2015 report jointly published by the International Telecommunication Union (ITU) and ABI research. Within this report there are five areas of analysis: the legal framework, the available technology, organizational structure, design capabilities and cooperation. Based on the analysis of these five elements, six countries in Latin America and the Caribbean have been selected in order to identify the strengths and weaknesses of the region. After briefly examining Brazil, Colombia, the Dominican Republic Guatemala, and Jamaica, we will have a better understanding of the current cybersecurity climate in Latin America.

Categorizing an attack based on the vulnerability of the aforementioned objectives could put a system at risk. Availability attacks refer to overwhelming a site with visits through denial of service (DoS) and even taking it offline to shut down physical aspects that depend on virtual processes. Confidentiality attacks are efforts made in order to gain access to a computer network to monitor activities and extract information on the system and on user data. The value of this attack is measured by the information obtained and the scope of the action. Integrity attacks involve entering the system to change rather than extract information; the idea is to manipulate information in the virtual world as well as the system and people who depend on that data in the real world.

In the context of cyber security according to the *Global Cybersecurity Index & Cyberwellness Profiles* report we have learned that most Latin American countries have legislation to control and oversee cyberspace activities, as well as some level of organizational structure. Regardless, there are important limitations in the area of policy, technology, coordination, and capabilities to combat illegal activities that may occur in cyberspace.

After the 9/11 attacks, the House of Representatives and the US Senate overwhelmingly approved the Patriot Act (Uniting and Strengthening America by Providing Tools Required to Intercept Appropriate and Obstruct Terrorism) giving full powers to intelligence gathering practices with little or no prior judicial control. However, on June 2, 2015, U.S Congress passed the USA Freedom Act which limits the Patriot Act and other instruments linked to intelligence gathering and management. However, many laws in Latin America are share many similarities with the Patriot Act which gave full power to the U.S government to practice and collect information with little or no prior judicial control.

Legal framework

These achievements in legislation at the national and institutional levels in Latin America have not resulted in a coherent cybersecurity strategy or action plan and it seems unlikely that this situation will improve in the short term. At the same time, several Latin American countries have constructed complex and diversified organizational structures between cybersecurity and cyber-defense and made major investments in financial, human, and material resources. Yet interagency coordination at the national and international level requires much more work.

Cybersecurity policy and strategy requires the implementation of a cyber-defense policy framework that would enable the protection of information related infrastructure and communications systems that support organizational structure. In addition, these policies and strategies should reinforce the missions and operations of security and defense institutions, as well as other state institutions charged with matters of national security.

Cooperation

Another area of vital importance is cooperation at the regional level so as to share developing capabilities for a common cyber security and cyber defense policy. For instance, a communications policy should be created that is geared towards raising the population's cybersecurity awareness so that they can act in a proactive and informed manner. This would help minimize the spread of cyber threats among internet users. Clear and specific guidance for cyber incident management should also be provided.

The cyberspace world finds itself in the private domain because of financial, human, material and technological resources, yet it requires the promotion of civil-military cooperation. In this way, synergy could be achieved between public agencies and the private sector via a public-private partnership (PPP) that supports policies and strategies for cybersecurity and defense at national, regional, and international levels. This task requires a centralized management command with a decentralized decision-making process in order to meet the threat and challenges found in the cyber domain.

Though several Latin American countries have developed or are involved in developing training programs in the field of cyber defense, the nature of the threat, as well as transnational crime, is borderless and characterized by its multidimensionality. Consequently, cooperation is necessary in order to address these threats and challenges in an efficient and effective manner. In this vein, once a policy of regional cybersecurity is established, states must engage in capacity building through training programs and joint training exercises within this common field for the sake of defending and protecting the region from cyber-attacks.

Another important and urgent aspect is the development of confidence-security-building measures for cybersecurity in the region. In this sense, the development of joint educational and training programs is necessary. A public-private partnership for the development of a plan, and educational programs and cybersecurity training is critical. Regional and sub-regional organizations under the leadership of the Organization of American States (OAS), such as the Union of South American Nations (UNASUR), the Central American Integration System (SICA), CEFAC, CDS, and others should begin discussions to develop a joint operational strategy for the region's common cybersecurity and defense. More than good will is required for the construction of a cyber-defense system at the regional level, and legislation, training and collaboration are necessary components. These achievements at the institutional level must be accompanied by the involvement of all states in the region, a clear definition of responsibilities, mutual trust, and the development of cyber defense capabilities, in addition to coherent operational plans.

It seems that cybersecurity legislations in Latin America are contrary to what happens in the United States and even in Europe where serious questions exist about safeguarding the fundamental rights and freedoms of citizens in this age of information and expression. In the region, no greater protection of cyberspace has been achieved through the expansion of government authority and intrusive legislations that affect the privacy of individuals.

In order to preserve democratic governance and protect citizens against the actions of their own government, we should reform the judiciary by giving it more and better resources rather than simply referring it to after violations of privacy in information and communications occur. Failure to do so would replicate the immediate response taken by the United States after September 11, 2001, which ignored the system of checks and balances of American democracy. Intrusive laws and greater authority for government action presents a complex and worrisome trend. It would be prudent to remember the words of Benjamin Franklin when he said, “They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety”.

Technology

Another aspect we must consider is that the cybersecurity system is heavily dependent on the talent and technology found in the private sector. With this in mind, there is a trend towards the militarization of cybersecurity due to its relationship with the defense and security sector. This raises serious questions that must be answered. For one, is the military with its current configuration on training, resources, and talent able to meet the threat and challenges of actors that move almost infinite resources and buy the talent needed? Second, is the career profile system of military forces and their capabilities adapted to the possibility of a confrontation in cyberspace? Third, and perhaps most important and in urgent need of answer: is there collective social talent and will it be incorporated into the military for the defense of the nation’s cybersecurity when needed?

The vast majority of military and civilians in the region would agree that we must respond negatively to the first question. This is the result of budgetary cuts that have hit the defense sector in recent years, as well as reduced recruitment and training of specialized military talent in cybersecurity and emerging technologies. It is generally not possible with the current military situation to perform the task of cyber defense with efficiency and efficacy, nor is it currently possible to ensure the sovereignty of the nation’s cyberspace which may have potential impacts on other traditional domains related to national defense and security.

With respect to the second question, we believe that we must introduce substantial improvements. Operating in cybersecurity requires a long career focusing and specializing in knowledge and experience. This should occupy a substantial part of the education curriculum of the officers and NCOs assigned to this domain. We cannot simply make use of personnel drawn from other units who are then allocated to specialized units in cybersecurity. It is a bad policy that results in inefficiencies and it is dangerous for the mission. Additionally, the policy should consider an appropriated professional profile, specializing in knowledge and experience in order to make it attractive and acquire new talent. We should keep in mind that the level of responsibility in protecting citizens and critical infrastructure is 24/7 and based on new rational thinking (knowledge and a high-level of expertise), this differs from traditional ways of defense used in other domains.

The answer to the third question allows for optimism. Most countries in the region have exceptional talent within their millennial generation, yet much of them have immigrated to other countries looking for opportunities to work for allies and even potential adversaries. We are paying a social waste. Nonetheless, there is still enough talent to give us an optimistic and positive answer to this last question. If we agree that this is true, then we must think about how to tap into the current generation's best talent so that there is even more talent in the future and participation in the nation's cybersecurity.

Structural organization

Creating a legal body that regulates the rights and obligations of the cybersecurity field should be a priority for any government and state policy in cybersecurity simply cannot be detached. This proposal is based on the citizens' obligation to institutional loyalty and mutual respect for cybersecurity leading to the creation and enhancement of a parallel structure—a command and control in which citizens' offer their participation. A Cybersecurity Reserve Corps of well qualified men and women should be offered basic military training so that they are able to understand the concept and functioning of the hierarchical structure of decision making processes and their participating scope.

This cyber reserve body must have horizontal channels of continuous relationship with their professional military counterparts for generating knowledge networks, organizational professional contacts, and exchange of knowledge and experience. This would enable rapid organizational integration under emergency situations. In the near future, there should be a body of regulation governing the powers of this cyber reserve in a clear, simple, and direct manner. It would not be good idea to opt for the Voluntary Reserve model as it works for other defense domains currently in force. The basic guidelines of the proposed cyber reserve model is based on Ávila's (2015) article, "Ciberreserva: Una necesidad estrategica para la defense nacional" (Cyber-reserve: A necessary strategy for national defense) which includes:

1. Establishment of cooperative systems for command and control training
2. Sharing information for proper deployment and activation in case of threat or conflict
3. Generating a recruitment system of new talent
4. Developing a recruitment system that permits at first glance those talents in order to compete in favorable terms
5. Model of integration for special situations under threat or conflict to minimizes inefficiencies and unwanted competition
6. Definition of an operating model of training while working to enable personnel operation competences for continuous readiness capabilities improvement

Latin American nations with limited talents in digital technology or economic and technological resource constraints will be able to make tremendous progress in cybersecurity within a generation's application of a proper model that takes legislation, structural organization, capability design, technology, means of cooperation at national and international levels and use of PPPs into consideration. Taken as a whole, these measures will provide cybersecurity under the main objectives of information security in terms of availability, confidentiality, and integrity.

If we realize that current thoughts on security and defense have lost their validity at the end of the twentieth century, and we think that we could be a technological region and that our reliance on information technology, either consciously or unconsciously, has finished, we as a region will understand the need to accept that the cyber domain must be defended with the utmost rigor and dedication.

Capabilities

In thinking about cybersecurity, we should overcome our proverbial trend toward disintegration and national interest by putting forth available talent so that it may become a collective talent oriented towards the security and defense of our cyber space made possible through the creation of a model heavily dependent on technology, energy, and wealth. We will be able to design a Cyber Reserve in which citizen participation in Cyber becomes necessary and indispensable and where its' numerous contributions result in the fruits of creation over the near future and long term, then certainly, these goals will become tangible.

The industrialization of digital technology in our region is necessary. Current dependence in this area of technology for cybersecurity is not desirable, even if today's trusted allies are reliable. Digital technology generates higher value in the field of research, development, and investment. This open citizen participation reveals the possibility for developing new models of production, which in turn induces a multiplier value in all economic areas. At the same time, civilian expertise in areas related to cybersecurity and protection of critical infrastructure would shift to our Armed Forces, enriching their experience and knowledge in this field and generating new social value and technological independence in the region.

The following analysis of cybersecurity in Latin America and the Caribbean has been made possible thanks to the information contained in the *Global Global Cybersecurity Index & Cyberwellness Profiles* April 2015 report published by ITU and ABI-research. We selected a group of countries in the region ranging from the most advanced to the less advanced in order to give a more approximated vision of the region's cybersecurity status, including its strengths and weaknesses, and the potential forms of action to improve this area of security and defense which has become one of the greatest global concerns and an inescapable reality for Latin America and the Caribbean.

The following pages will present you with a group of countries that have made tremendous investment in all kind of resources such as talent, financial investment, technology, organizational structure, capacity, and some kind of cooperation at the national level. However, there is still a lot of work to be done in all these areas. The major change, however, is in the mode of thinking [out of the box] about cybersecurity in order to develop a regional system capable of protecting not only our cyberspace, but the impact of that domain on the region's security, defense, institutions, and citizens as a whole.

Brazil

In 2012, Brazil adopted the White Paper to Guide Future Defense Priorities and since then the country has quickly built up an impressive cybersecurity institution in addition to outsourcing most responsibility for the country's cybersecurity to the Army's Center for Cyber Defense (CDCiber). Established in 2012, CDCiber's declared purpose is for defense and it is better funded and organized compared to other public institutions that combat cybercrime such as the Federal Police. Taken as a whole, Brazil has not only laid down the groundwork, but carries the political will to be at the forefront of cybersecurity and defense given its continual rise as a global player. As indicated by Canongia and Mandarino (2014), "Although this [security] framework is recent, when compared to the framework of laws, norms and standards of developed countries, it is acknowledged nationally and internationally for its competent structure to handle matters directly correlated with cyber security" (p. 71). While Brazil's "Internet architecture" is still a work in progress, Dinniz, Muggah, and Glenny (2014) argue that the country's current cybersecurity strategy is "narrowly focused" on foreign threats and overly concerned with strengthening cyber war-fighting and anti-terrorism capabilities. This consequently ignores real and ongoing cybercrime, leading to an imbalance in their security approach. For instance, cybercrime such as the spread of viruses or malware and bank fraud, costing the country around $8 billion annually, has drastically risen in Brazil since 2006. Further estimates suggest that Brazil is third most affected by illegal digital activities worldwide (Dinniz, Muggah, & Glenny, 2014). One distinguishing characteristic of Brazil's Internet landscape worth mentioning is the country's high use and production of social media. For instance, "Almost 60 per cent of Internet users in Brazil are registered on Facebook, second only to the United States in number of profiles . . . Globally, Brazil is fifth in overall in Twitter use." (Dinniz, Muggah, & Glenny, 2014, p. 6). After the 2013 protests, CDCiber and Brazil's central intelligence agency (ABIN) created controversial social media monitoring platforms, such as Mosiac, in order to track and monitor protests.

Colombia

In a way, Colombia has acted as a regional leader in cybersecurity thanks to guidance and support from the OAS. For instance, in 2009 Congress passed a new law that created and defined criminal offenses specific to cybercrime. Then in 2011, Colombia became the first country in Latin America to create a comprehensive cybersecurity and cyber defense strategy (CONPES 3701) resulting in the formation of specialized government (colCERT), police (Police Cyber Center) and military forces (Joint Cyber Command). On top of this, the Colombian government and Microsoft signed a memorandum of understanding to develop ICTs in the areas of cybersecurity, education and innovation and in 2013, Microsoft opened an Anti-Cyber Crime Office in Bogotá as its Latin American outpost (Parkinson, 2013; Volckhausen, 2013; Volkert, 2013). In 2014, President Juan Manuel Santos requested that the OAS send a team of international experts in order to assist the country in developing a new cyber defense strategy. As a result of OAS recommendations, Colombia created the National Cyber Security Agency and the Digital Committee. Regardless, Colombia still faces a high degree of cybercrime, particularly in the form of credit card fraud, phishing and hacking. For instance, in 2013 Colombia was ranked as the worst country in Latin America and eighth in the world for phishing, resulting in losses of $95 million (Yagoub, 2014).

Dominican Republic

While the Dominican Republic has specific legislation that prosecutes cybercrime and several organizations that investigate cybercrimes such as the National Police and the Cybercrimes Investigation Division (DIDI), there is a fundamental weakness to its cybersecurity approach. This is precisely because it lacks an overarching national policy and strategic framework in regards to cybersecurity, as well as technical expertise (ITU, 2015; OAS, 2014a). On the other hand, the OAS (2014a) praised the Dominican Republic for improving cooperation with other countries, as seen in several multi-lateral operations. The Dominican Republic was also the first country in Latin America and the Caribbean to ratify the Council of Europe's Convention on Cybercrime. Internet usage amongst the population continues to grow, but so does (unsophisticated) cybercrime, particularly in the form of credit card cloning, digital identity theft, and phishing, as well as defacement of government websites by hacktivists (OAS, 2014a).

Guatemala

In 2009 Guatemala established cybersecurity and cybercrime legislature with the aim of preventing and prosecuting cybercrimes and protecting data. However, Guatemala's current cybersecurity system contains many gaps and weak spots as a result of no national cybersecurity strategy. Further problematic is the lack of a national computer security incident response team (CSIRT), despite the existence of a private sector one. As described by the OAS (2014a), “Cooperation between Guatemalan authorities and their counterparts outside of the country is limited and generally occurs in an informal and ad hoc fashion, between persons or offices where contacts have been made through participation in regional workshops or other activities. Such engagement is limited primarily to entities in Central America and the Caribbean” (p. 57) However, there are several indications that Guatemala has begun to branch out and address its cybersecurity situation more seriously. For instance, in June 2014 the OAS and the Guatemalan government engaged in a Cyber Security Symposium attended by experts from the National Police of Colombia, the National Polytechnic Institute of Mexico and the OAS’ Inter-American Committee against Terrorism (CICTE) which promotes the use of CSIRTs as a sort of ‘hemispheric alert network’ and now Guatemala is in the process of designing an official CSIRT (OAS 2014a; OAS, 2014b). Even more, the country is reportedly developing a national cybersecurity strategy which will help to bridge the many cybersecurity gaps still present (OAS, 2014a).

Jamaica

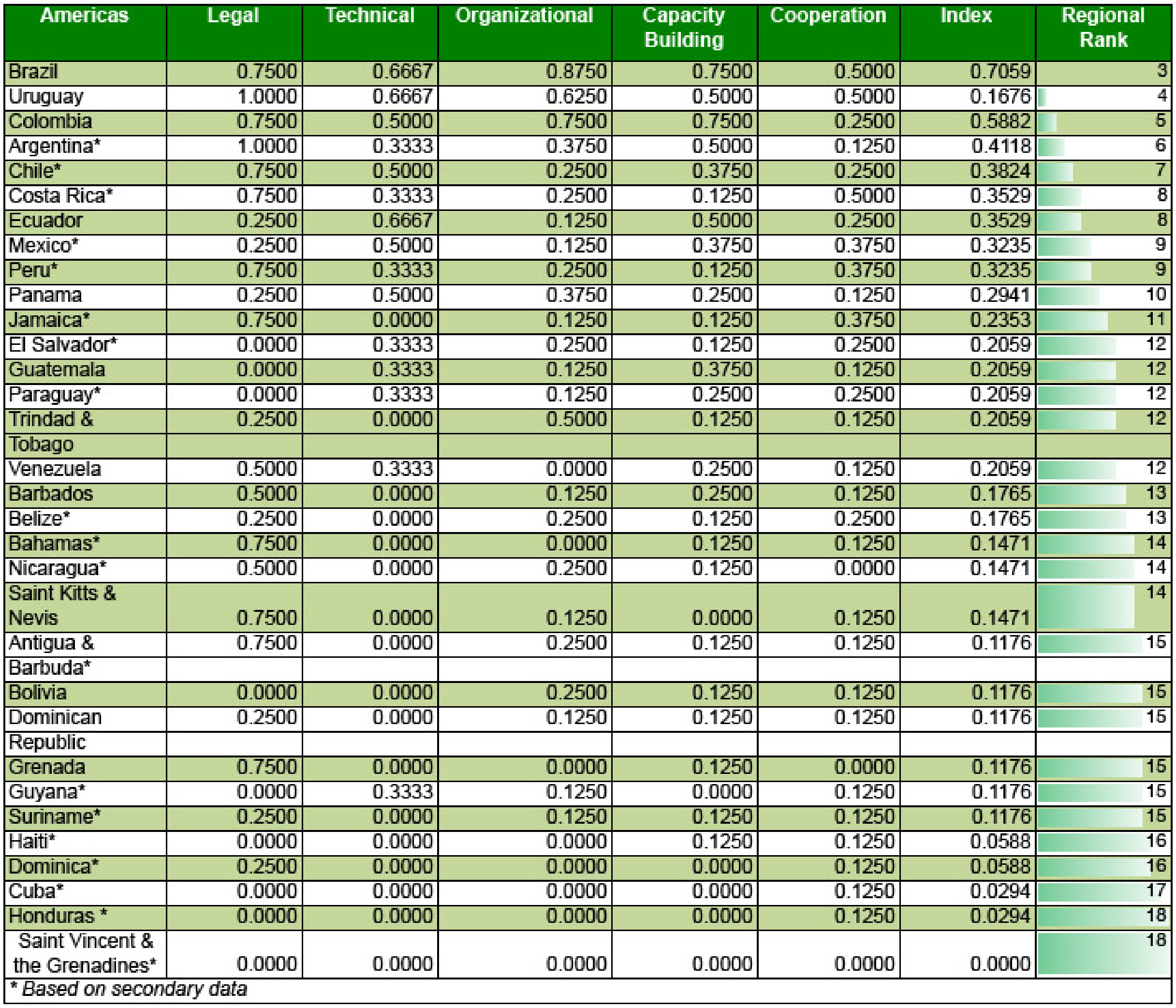
In 2012, Jamaica revised its cybercrime legislation, began establishing a computer security incident response team (CSIRT) and expanded its Communication Forensic Unit (CFCU). At the same time, the number of cyber incidents increased. According to the OAS (2013), “The growing frequency of cyber incidents in Jamaica is complicated by the lack of highly trained incident response and digital investigation personnel, inadequate domestic and international cooperation, and a lack of proactive measures to deter hackers and attackers” (p. 7). However, since 2014 Jamaica has taken strides to address its weak cybersecurity. For instance, the Cyber Security Programme, which is an OAS mandated program that assists member states in developing cybersecurity capabilities and policy frameworks, began providing technical support to the Jamaican government in regards to the development of a national cybersecurity plan. This resulted in the formation of a National Cyber Security Strategy (NCSS) which was unrolled to the public in February, 2015. Yet according to Marius (2015), “It [NCSS] still appears somewhat superficial, in that it has little depth: a general course has been plotted, but much still needs to be fleshed out. To some degree, this approach could be attributed to the fact that cybersecurity is a new area, and the since most of players would have little experience in that space, the strategy has been designed to given them, and the entire process, some latitude to adjust as needed” (n.p.).

Mexico

The Federal Police of Mexico is the main authority for cybersecurity and cyber-related efforts in Mexico, though other government institutions actively participate alongside them. Within the Federal Police of Mexico is the Scientific Division, a highly trained unit whose “Emphasis is placed on securing instruction to ensure that personnel are trained in accordance with their specific responsibilities, and that their knowledge and skills are as up-to-date as possible” (OAS, 2014a, p. 64). This specialized training comes from domestic sources as well as international law enforcement organizations from countries such as Colombia, the US, Holland and Japan (OAS, 2014a). The Scientific Division houses the country’s head CSIRT, called CERT-MX. CERT-MX is charged with many high level responsibilities including the protection of critical infrastructure. Despite these positive aspects, the OAS asserts that a lack of legislation keeps law enforcement from effectively responding to cyber threats. To elaborate, “The limited capacity of law enforcement to act in many instances undermines investigations, perpetuates a sense of impunity among organized criminal groups, and enables the latter to deploy the latest technologies and techniques to commit crimes.” (OAS, 2013, p. 65). Cybercrime trends in the country include phishing, hacking, the spread of malware and in 2013, the Mexican economy lost 3 billion as a result of cybercrime (Sonneland, 2015). Lack of public awareness is another major factor that contributes to Mexico’s cyber insecurity.

In the following table on page 9 it is a summary of Latin American and Caribbean countries in rank order based on the index created by the *Global Cybersecurity Index & Cyberwellness Profiles* April 2015 report published by ITU and ABI-research. Available in References.

Latin America & Caribbean Ranking by Index



Americas	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Brazil	0.7500	0.6667	0.8750	0.7500	0.5000	0.7059	3
Uruguay	1.0000	0.6667	0.6250	0.5000	0.5000	0.1676	4
Colombia	0.7500	0.5000	0.7500	0.7500	0.2500	0.5882	5
Argentina*	1.0000	0.3333	0.3750	0.5000	0.1250	0.4118	6
Chile*	0.7500	0.5000	0.2500	0.3750	0.2500	0.3824	7
Costa Rica*	0.7500	0.3333	0.2500	0.1250	0.5000	0.3529	8
Ecuador	0.2500	0.6667	0.1250	0.5000	0.2500	0.3529	8
Mexico*	0.2500	0.5000	0.1250	0.3750	0.3750	0.3235	9
Peru*	0.7500	0.3333	0.2500	0.1250	0.3750	0.3235	9
Panama	0.2500	0.5000	0.3750	0.2500	0.1250	0.2941	10
Jamaica*	0.7500	0.0000	0.1250	0.1250	0.3750	0.2353	11
El Salvador*	0.0000	0.3333	0.2500	0.1250	0.2500	0.2059	12
Guatemala	0.0000	0.3333	0.1250	0.3750	0.1250	0.2059	12
Paraguay*	0.0000	0.3333	0.1250	0.2500	0.2500	0.2059	12
Trindad & Tobago	0.2500	0.0000	0.5000	0.1250	0.1250	0.2059	12
Venezuela	0.5000	0.3333	0.0000	0.2500	0.1250	0.2059	12
Barbados	0.5000	0.0000	0.1250	0.2500	0.1250	0.1765	13
Belize*	0.2500	0.0000	0.2500	0.1250	0.2500	0.1765	13
Bahamas*	0.7500	0.0000	0.0000	0.1250	0.1250	0.1471	14
Nicaragua*	0.5000	0.0000	0.2500	0.1250	0.0000	0.1471	14
Saint Kitts & Nevis	0.7500	0.0000	0.1250	0.0000	0.1250	0.1471	14
Antigua & Barbuda*	0.7500	0.0000	0.2500	0.1250	0.1250	0.1176	15
Bolivia	0.0000	0.0000	0.2500	0.1250	0.1250	0.1176	15
Dominican Republic	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	15
Grenada	0.7500	0.0000	0.0000	0.1250	0.0000	0.1176	15
Guyana*	0.0000	0.3333	0.1250	0.0000	0.1250	0.1176	15
Suriname*	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	15
Haiti*	0.0000	0.0000	0.0000	0.1250	0.1250	0.0588	16
Dominica*	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	16
Cuba*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	17
Honduras *	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	18
Saint Vincent & the Grenadines*	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	18

** Based on secondary data*

Note. Adapted from *Global Cybersecurity Index & Cyberwellness Profiles* p. 9-10, by ITU-ABIresearch 2015, Geneva: Telecommunication Development Bureau.

Conclusions

As we look into the future—its promises and its challenges—we are facing a brave new world, the most fast-paced and exciting period in human history. We'll experience more change at a quicker rate than any previous generation, and this change, driven in part by the devices in our own hand, will be more personal and participatory than we can even imagine. Computation, the backbone of every technology we can see today, behaves in much the same way. Even with its eventual inevitable limitations, Moore's Law promises us infinitely smaller processors in just a matter of years. Every two days we create about five exabytes of information with only two billion people out of the possible seven billion online (Schmidt & Cohen, 2013). How many new ideas, new perspectives and new creations will truly global technological inclusion produce? In the future, information and communication technology will be everywhere like electricity.

Confidentiality, availability and integrity appear to be the three main objectives in the development of computer security systems and if we don't pursue the highest technological standards these areas become a source of vulnerability to any offensive action. As we mentioned, availability attack could shut down the physical or virtual process that depend on it, a confidentiality attack could allow criminals to access valuable information that might endanger institutions and individuals, and an integrity attack would allow criminals to exchange information to manipulate processes in the virtual world as well as the systems and people that depend on it. Additionally, the five key areas of legislation, technicality, organization, capacity building, and cooperation matter greatly to the future story of cybersecurity. Indeed none of these areas are definite and there will be many more that will emerge with the development of new technology. However, these areas are driven by a number of factors that we should begin to observe. Additionally, these five areas should act as bases of analysis in order to begin serious and urgent preparation for cyberspace use under government control and oversee, including acceptable government empowerment and exercise of surveillance on their people within the cyber domain.

The legal framework, is one of the areas where most countries have made some progress in order to control human behavior by providing rules for basic conduct when this domain is used; second, the area of available technology is more limited at this time because of the lack of human capital capable of developing new digital technology to put it into practice; third, organizational structure for the execution of defense/offense operations in general needs to be better coordinated; fourth, designing capabilities according to the mission requirements is an area that requires a lot of work; and cooperation throughout the development of confidence-security building measures should be created so as to provide a level of security with the best available capacity in the region.

In Latin America, cyberspace is fragile and vulnerable in availability, confidentiality, and integrity. In order to develop a cybersecurity system capable of ensuring acceptable state control of this domain, a public-private partnership model should be used. The overwhelming participation of technology, human resources and financial support in the private sector will be instrumental for the development of capabilities according to the threats and challenges that must be confronted. Cooperation is the principle tool that should be applied if we want to have a firm and strong cyberspace.

Another task required is designing a policy and strategy based on the nature of this new domain and the technology available. This must take into account human capital, financial resources, enacted laws, and the regulated security standards of banks, public utilities, and other critical infrastructures. In order to have efficiency and efficacy for an integrated policy and strategy in this domain's management, the Security and Defense Institutional Building (SDIB) model should be applied. This model will enable the system to protect the information and communication systems of the infrastructure that support the organizational structure, mission and operations of the institutions of security and defense as well as other state and private institutions in charge of security in the nation.

A regional policy on cybersecurity should be established, this policy requires that states engage in capacity building through training programs and joint training exercises in the common policy field of defense and protection for the region's cyberspace. At the same time, it should be decided which institutions will be responsible for the security and defense of cyberspace in order to develop a common doctrine with a quality-oriented service criteria for security and defense of the region's common interests.

At the beginning of this paper we explained and analyzed the five characteristics of cybersecurity, and the three major vulnerabilities of the information and telecommunication systems. Yet it is the private sector who will be responsible for most innovation in cybersecurity—the government will never be able to offer competitive wages to skilled technology workers. The dilemma is how much relative weight we give to security in cyberspace, and who should be responsible for it.

But cyberspace is too vast, and too pervasive to allow a single entity to govern it or to dictate the norms of behavior. There is no net way to define cyberspace. It is not a common, but a private. We have come to depend on it as a public utility—like electricity and water. But it mostly remains a collection of privately owned devices. Fortunately, we are at the dawn of the new age, not its twilight, and there is time to consider this conundrum which has confounded every discussion about the nature of this space to which we seem inexorably tied.

Time is running short and new technologies and applications will emerge that will revolutionize our conceptions, just as the explosive growth of cyberspace over the last two decades has upended much what we knew about security. Governments in Latin America and corporations are making the rules as they go, and their actions have had a more tangible effect than many have realized. Cyberspace is incumbent on everyone who touches it in the region—an undeniable collective. Eisenhower's (1961) declaration, ". . . to find essential agreement on issues of great moment, the wise resolution of which will better shape the future of the nation" captures the essence of the need for collective contribution.

References

Ávila, E. (2015). "Ciberreserva: una necesidad estratégica para la defensa de la nación". *CIBER Elcano Nº 5* (p.11). Real Instituto & THIBER. Retrieved from http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciber-elcano-05-julio-2015#.VZ65Jj8w-os

Canongia, C. & Mandarino, R. Jr. (2014). "Cybersecurity: The New Challenge of the Information Society". *In Information Resources Management Association* (Ed.) Crisis Management: Concepts, Methodologies, Tools, and Applications (p. 60-80). Hershey, PA: Information Science Reference.

Dearth, D. H. (2000). *Cyberwar 3.0 Human Factors in information Operations and Future Conflict.* Fairfax, VA: Armed Forces Communications and Electronics Association (AFCEA) International Press.

Diniz, G., Muggah, R. & Glenny, M. (2014). *Deconstructing Cyber Security in Brazil: Threats and Responses (Strategic Paper 11)*. Rio de Janiero, Brasil: Igarapé Institute. Retrieved from http://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf

Eisenhower, D. D. (1961) Military-Industrial Complex Speech. Yale Law School Lillian Goldman Library. Retrieved from http://avalon.law.yale.edu/20th_century/eisenhower001.asp

Franklin, B. (n.d.). Benjamin Franklin Quotes. Brainy Quotes. Retrieved from http://www.brainyquote.com/quotes/quotes/b/benjaminfr136955.html

Harris, S. (2014). *@War The Rise of the Military-Internet Complex.* New York, NY: Eamon Dolan/Houghton Mifflin Harcourt.

International Telecommunications Union & ABIresearch (2015). *Global Cybersecurity Index & Cyberwellness Profiles*. Geneva, Switzerland: Telecommunication Development Bureau. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

Muggah, R. & Glenny, M. (2015). Guest Post: Brazil's Cybersecurity Conundrum. Council on Foreign Relations. Retrieved from http://blogs.cfr.org/cyber/2015/01/12/guest-post-brazils-cybersecurity-conundrum/

Organization of American States (2013). *Latin American and Caribbean Cybersecurity Trends and Government Responses*. Cupertino, CA: OAS & Trend micro. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Organization of American States (2014a). *Latin American and Caribbean Cybersecurity Trends.* Washington, DC: OAS & Symantec. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Organization of American States (2014b). OAS and Guatemala Begin Cyber Security Symposium. OAS. Retrieved from http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-242/14

Parkinson, C. (2013). Microsoft opens anti-cybercrime office in Colombia. Insight Crime. Retrieved from http://www.insightcrime.org/news-briefs/microsoft-establishes-anti-cyber-crime-presence-in-colombia

Reagan Ronald, President of United States of America 1981-1989 http://www.brainyquote.com/quotes/quotes/r/ronaldreag100997.html#oWGUtORutrAtRRx3.99

Real Instituto Elcano & THIBER (2015). Ciber elcano Nº5: *Ciberreserva: Una necesidad estrategica para la defensa de la nacion*. Real Instituto Elcano de Estudios Internacionales y Estratégicos & THIBER.

Schmidt, E. & Cohen, J. (2013). *The New Digital Age: Reshaping the future of people, nations and business*. New York, NY: Random House, Inc.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press.

Volckhausen, T. (2013) Microsoft opens office in Colombia to fight Latin America cybercrime Colombia Reports. Retrieved from http://colombiareports.com/microsoft-opens-office-colombia-fight-latin-american-cyber-crime/

Volkert, Z. (2013). Microsoft to bring ICT innovation to Colombia. BN Americas. Retrieved from http://www. Bnamericas.com/news/technology/Microsoft-to-bring-ict-innovation-to-colombia

Yagoub, M. (2014). Cyber Crime in Colombia: An Underestimated Threat? Insight Crime. Retrieved from http://www.insightcrime.org/news-analysis-crime-colombia-understimated-threat

William J. Perry
Center for Hemispheric Defense Studies
National Defense University
Abraham Lincoln Hall
260 5th Ave. Bldg. 64
Washington, DC 20319-5066