# Document Conpes

**3701**

National Council on Economic and Social Policy

Republic of Colombia

National Planning Department

**POLICY GUIDELINES ON**
**CYBERSECURITY AND CYBERDEFENSE**

Ministry of the Interior and Justice

Ministry of Foreign Affairs

Ministry of Defense

Ministry of Information and Communication Technologies

Department of Security Administration

National Planning Department-DJSG-DIFP-DIES-OI

Office of the Attorney General

Version: Draft

Bogotá D.C., July 14$^{Th}$ of 2011

Summary:

The purpose of this document is to generate policy guidelines on cybersecurity[1] and cyberdefense[2] with the aim of developing a national strategy to counter the rise in cyber threats that have significant impact on the country. In addition, it examines past experiences, both within the country and abroad, as well as the country's legal framework on the subject.

The core issue hinges on the fact that the state's current capacity to confront cyber threats is hampered by weaknesses and the lack of a national strategy in this area. Based on the foregoing the causes and effects have been identified from which to develop prevention and control policies against the increase in cyber threats. In order to enable the strategy's implementation, this document offers specific recommendations for entities directly and indirectly involved in this issue. This was the position that the Colombian government adopted when it included this issue in the *Plan Vive Digital* [Live Digital Plan] within the framework of the 2010-2014 National Development Plan "Prosperity for All."

**Classification:** H011, H411, R011

**Keywords:** Cyber threat, cyberspace, cyberdefense, cybersecurity, information security, critical infrastructure, CERT, ColCERT.

1. The state's capacity to minimize the level of exposure of its citizens to cyber threats or incidents.
2. The state's capacity to prevent and counter any cyber threat or incident that undermines national sovereignty.

**CONTENTS**

# I. INTRODUCTION

The use of information and communication technologies brings with it changes and permanent threats and has become one of the cornerstones of the globalized world. At the same time, the evolution of these technologies has brought an increase in the use of technological resources for criminal purposes all over the world.

The continual evolution, spread, and sophistication of cyber attacks, as well as technological convergence,[3] highlight the need to adopt measures and controls to protect the state from these new threats.[4] The increased capacity to commit crime in cyberspace as well as the use of new technologies to generate cyber threats, constitute a common concern for all countries, given that they significantly impact information security in both public and private spheres, including civil society.

Tackling the issues of cybersecurity and cyberdefense entails a commitment on the part of the national government to guarantee information security. Therefore, although this document aims to provide a policy framework for the issues of cybersecurity and cyberdefense in particular, the entities involved will be responsible for developing that framework and creating mechanisms by which to ensure information security nationwide. To achieve the foregoing, consideration will be given to technical rules and national and international standards, as well as international initiatives on protection of critical infrastructure and cybersecurity.

Bearing in mind that the government needs to be aware of and act comprehensively against cyber threats, a strategy is needed that includes the creation of appropriate bodies to perform the task of providing cybersecurity and cyberdefense against any cyber threats or incident that could

---

3. Technological convergence is the tendency for different technological systems to evolve towards performing similar tasks. Convergence can refer to previously separate technologies such as voice (and telephony features), data (and productivity applications), and video that now share resources and interact with each other synergistically (Jenkins, Henry (2006) Convergence Culture, New York University Press, New York).

4. A potential cause of an unwanted incident, which may result in harm to a system or organization. (ISO/IEC 13335-1:2004).

compromise information,[5] impair the country's critical infrastructure, and jeopardize the security and defense of the state. The adoption of a national policy on cybersecurity and cyberdefense involving all sectors of society, under the leadership of the Ministry of Defense and in coordination with other state entities, is an imperative of the highest priority.

This document identifies as the overarching objective of this policy the strengthening of the state's capacity to confront cyber threats to its security and defense. It also defines three specific objectives: 1) To implement appropriate mechanisms to prevent, provide assistance, control, and offer recommendations on cyber incidents and/or emergencies for protecting the country's critical infrastructure; 2) To design and execute specialized cybersecurity and cyberdefense training plans; and, 3) To strengthen the legal framework and law enforcement in this area.

This document sets out a plan of action for putting into effect the policy on cybersecurity and cyberdefense, which will be entrusted to the entities involved.

## II. BACKGROUND

In April 2007, the government of Estonia sustained what is generally regarded as the biggest cyber attack in history; it affected the office of the president, the parliament, most ministries, political parties, and two major banks. The attack triggered a crisis that necessitated the intervention of the international community and alerted NATO. As a result, in August 2008, NATO launched the Cooperative Cyber Defence Centre of Excellence (CCD COE), whose mission is to protect the Organization's members from attacks of this type, provide training to military personnel, conduct research on electronic defense techniques, and develop a legal framework for pursuing this activity.

---

5. Cyber threat: The appearance of a potential or actual situation in which an agent has the capacity to produce a cyber attack against the population, territory, and political organization of the state. (Ministry Of Defense Colombia)

   Cyber incident: One or a series of unexpected or unwanted cybersecurity events that have a significant probability of compromising the operations of an entity or threatening information security. (Ministry Of Defense Colombia)

There are two other significant cyber attacks that are also worth mentioning. The first was against the United States in July 2009, when a series of attacks affected the White House, the Department of Homeland Security (DHS), the Department of Defense, the Federal Aviation Administration, and the Federal Trade Commission.[6] The other event was that reported by Spain's Guardia Civil in March 2010, when it dismantled one of the largest so-called zombie computer networks,[7] known as the *mariposa* (or butterfly) botnet[8], composed of more than 13 million infected IP addresses[9] distributed across 190 countries. Colombia was the fifth worst-affected country by this network.

| No. | COUNTRY | % |
|---|---|---|
| **1** | INDIA | 19.14 |
| **2** | Mexico | 12.85 |
| **3** | BRAZIL | 7.74 |
| **4** | KOREA | 7.24 |
| **5** | **COLOMBIA** | **4.94** |
| **6** | RUSSIA | 3.14 |
| **7** | EGYPT | 2.99 |
| **8** | MALAYSIA | 2.86 |
| **9** | UKRAINE | 2.69 |
| **10** | PAKISTAN | 2.55 |

| No. | COUNTRY | % |
|---|---|---|
| **11** | PERU | 2.42 |
| **12** | IRAN | 2.07 |
| **13** | SAUDI ARABIA | 1.85 |
| **14** | CHILE | 1.74 |
| **15** | KAZAKHSTAN | 1.38 |
| **16** | UNITED ARAB EMIRATES | 1.15 |
| **17** | MOROCCO | 1.13 |
| **18** | ARGENTINA | 1.10 |
| **19** | UNITED STATES | 1.05 |

TABLE 1: Latin American countries worst affected by a zombie network in March 2010
Source: www.infospyware.com

---

6. Report to Congressional Requesters, United States Government Accountability Office, March 2010, http://www.gao.gov/new.items/d10338.pdf

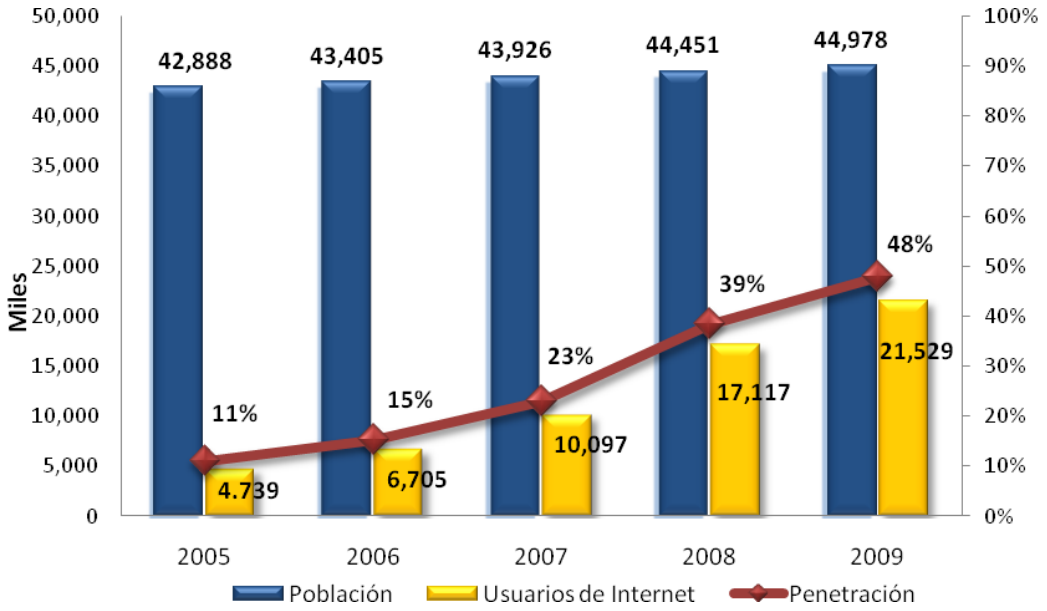
7. Term used to refer to personal computers which, after being infected by some type of malware, can be used by a third party to carry out hostile activities. This use occurs without the consent or knowledge of the machine's user.

8. The name given to a network of computers that combines their resources to perform a common task and shares the workload among all the computers (FireEye – Arbornet). A botnet's originator can control the infected computers/servers remotely, usually through a means such as IRC: Newer versions of these botnets are focusing on control environments via HTTP, greatly simplifying control of these machines. Their purposes are usually nefarious.

9. A numerical label assigned, logically and hierarchically, to the interface (communication/connection element) of a device (normally a computer) within a network that uses the IP protocol (Internet Protocol). www.iso.org

As regards the private sector, a study found that the average cost to each company that was a victim of cyber attacks was US$2 million a year.[10] Of the organizations involved, 42% rated cybersecurity as their main priority, bearing in mind that 75% of them suffered some form of security breach in the 12 months prior to the study. Other factors that were identified as being critical to security were staff shortage, new information technology initiatives, and compliance problems with information technology standards.[11]

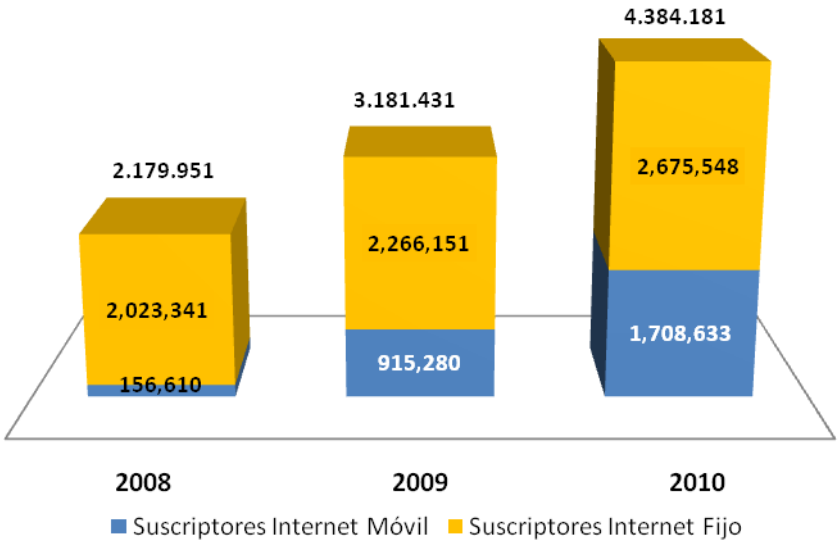
In Colombia use of information and communication technologies has increased significantly, raising the country's level of exposure to cyber threats. According to graph 1, the number of Internet users went up by 354% between 2005 and 2009. The number of Internet subscribers increased by 101% between 2008 and 2010, reaching a total of 4,384,181 fixed and mobile Internet subscribers. Of those, 39% are fixed subscribers and 61% are mobile subscribers, as graph 2 shows.




Graph 1. Internet users, 2005 - 2009
Source: Data reported by network providers and services to SIUST, DANE

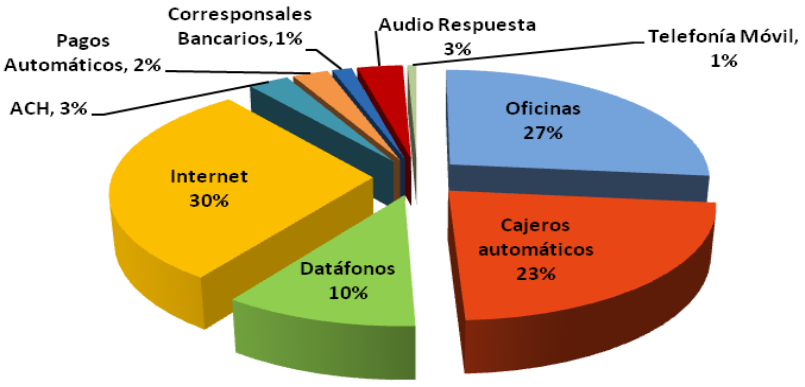
10. Source: http://www.symantec.com/es/mx/business/theme.jsp?themeid=state_of_enterprise_security

11. Source: http://www.symantec.com/es/mx/business/theme.jsp?themeid=state_of_enterprise_security




Graph 2. Internet subscribers, 2008 - 2010
Source: Data reported by network providers and services to SIUST

The Internet has become an increasingly popular medium among users of banking services. According to the Financial Superintendency of Colombia, in 2010, 30% of financial and non-financial transactions were carried out online, which, as graph 3 shows, represent an increase of 12% in the number of operations carried out using in this way compared with 2008.




Graph 3. Financial and non-financial operations, by medium, 2010
Source: Transactions and Operations Report, Financial Superintendency of Colombia

The value of financial operations conducted online in 2010 came to 1.237 billion pesos, which amounts to a rise of 121% compared to 2008.

As regards cybersecurity, Colombia has also been the target of attacks. One notable incident occurred in the first half of 2011 when the "hacktivist" group that calls itself Anonymous attacked the portals of the office of the president, the Senate, the online government portal, and the Ministries of the Interior and Justice, Culture, and Defense, leaving their websites off-line for several hours. The attack was launched in protest against a proposed law regulating responsibility for online infringements of copyright and related rights. This group has indiscriminately targeted public and private sector entities, including PayPal, the Swiss bank PostFinance, MasterCard, Visa, and Swiss government websites.

Also worth mentioning are the complaints that have also been reported by private citizens to the Colombian police. From January to December 2009, the police dealt with 575 cyber offenses recognized by Law 1273 of 2009.[12] These offenses included abusive access to a computer system (259), computer and related theft (247), data interception (17), violation of personal data (35), unauthorized assets transfer (8), website impersonation (5), computer damage (3), and unlawful obstruction of a computer system (1). In 2010, the number of offenses and infringements increased by 73%, to a total of 995 cyber offenses. The biggest increase came in the area of computer theft, where the number rose from 247 to 502,[13] equivalent to 103%.

### A. National Framework

In order to put Colombia's legal framework in perspective it is important to mention the country's lawmaking efforts in chronological order, as follows:

---

12 Law 1273 criminalized behavior connected with cyber offenses and information and data protection.

13. Data reported by the National Police's Crime and Operational Statistics System (SIEDCO)

| LAW / RESOLUTION | SUBJECT MATTER |
|---|---|
| Law 527 of 1999 - ELECTRONIC TRADE | Defines and regulates access to and use of data messages, electronic trade, and digital signatures, as well as establishing the certification entities and introducing other provisions." |
| Law 599 of 2000 | Enacts the Criminal Code. The Law maintains the structure of the definition of the crime of "unlawful violation of communications," recognizes copyright as a legal interest, and includes a number of conducts indirectly connected with cybercrime, such as the offer, sale, or purchase of an instrument apt for use to intercept private communications between persons. The Law also defined "Improper access to a computer system" as follows "Art. 195. Anyone who gains improper access to a computer system protected with a security measure or remains within same against the will of someone entitled to exclude them shall be liable to a fine." |
| Law 962 of 2005 | Introduces provisions on streamlining of administrative formalities and procedures of government agencies and entities, as well as of private persons who perform public functions or provide a public service. Provides for the incentive of using integrated technological mechanisms to reduce the time and cost of procedures for those subject to administration. |
| Law 1150 of 2007 | Introduces measures to encourage efficiency and transparency in Law 80 of 1993, and issues other general provisions on procurement using public funds. In particular, the law establishes the possibility for the public administration to issue administrative decisions, documents, and notices by electronic means, to which end it provides for the development of the Electronic Government Procurement System (SECOP). |
| Law 1273 of 2009 | Amends the Criminal Code and creates a new legally protected interest called information and data protection. The Law comprehensively protects systems that use information and communication technologies, among other provisions. |
| Law 1341 of 2009 | Defines principles and concepts relating to the information society and the organization of information and communication technologies (ICTs). This law also creates the National Spectrum Agency as well as issuing other provisions. |

| LAW / RESOLUTION | SUBJECT MATTER |
|---|---|
| Communications Regulation Commission resolution 2258 of 2009 | On network security of network providers and telecommunications services. This resolution amends Articles 22 and 23 of CRT resolution 1732 of 2007 and Articles 1(8) and 2(4) of CRT resolution 1740 of 2007. This rule recognizes the obligation for network providers and/or telecommunications services that offer Internet access to implement security models in accordance with the specific characteristics and needs of their network, in order to help improve the security of their access networks in keeping with the security frameworks defined by the ITU, abiding by the principles of data confidentiality, data integrity, and availability of network elements, information, services, and applications, as well as measures for authentication, access, and non-repudiation. It also establishes obligations to be met by network providers and telecommunications services in the area of communications inviolability and information security. |
| Circular 052 of 2007 (Financial Superintendency of Colombia) | Sets the minimum security and quality requirements on information management through goods and services distribution media and channels for clients and users. |

TABLE 2: Domestic standards

Different initiatives have been devised in a number of sectors, which CONPES has drawn on as research and reference papers for preparing this document:

| INITIATIVE | LEAD ENTITY | SCOPE |
|---|---|---|
| Information Security Model for the Online Government Strategy | Online Government Program - Ministry of Information and Communication Technologies | This security model is founded on the set of strategic policies that underpin online government, such as “protection of personal information" and “credibility and trust in online government.” It establishes the following as fundamental elements of information security for government agencies: 1) Availability of information and services. 2) Information and data integrity. 3) Information confidentiality. |

| INITIATIVE | LEAD ENTITY | SCOPE |
|---|---|---|
| Recommendations to the national government for implementing a National cybersecurity Strategy | Telecommunications Regulation Commission | In this document the Communications Regulation Commission offers the national government recommendations for the establishment of a National Cybersecurity Strategy; puts suggests suitable public-private collaboration and cooperation mechanisms; identifies ways to deter cybercrime; recommends the implementation and development of cybersecurity legal frameworks consistent with international standards; offers recommendations for the development of response systems for network security incidents, including surveillance, analysis, and incident response; and proposes guidelines for introducing a national cybersecurity culture in order to improve protection of critical information infrastructure in Colombia. |
| CSIRT- CCIT - Computer Security Incident Response Team for Internet service providers (ISPs). | Colombian Chamber of Informatics and Telecommunications (CCIT) | The Colombian Computer Security Incident Response Team, which is in direct contact with the security teams of its member companies (the largest Internet service providers in Colombia). It has the capacity to coordinate attention and response to any requests and complaints concerning computer security problems that it receives. |

Table 3: National initiatives

Furthermore, Colombian government agencies have been raising awareness about the importance of developing a cybersecurity and cyberdefense policy since 2007. To that end, the national government, in partnership at the international level with the Organization of American States (OAS), through the Inter-American Committee against Terrorism (CICTE), organized a workshop on cybersecurity awareness in May 2008, followed by a national roundtable in October 2009. As an upshot of the above activities, government agencies requested the Ministry of Defense to lead the way in implementing cybersecurity policies and establish mechanisms to respond to any cybercrimes and incidents that might affect the nation. This request arose as a result of the need for an in-depth analysis of the specific features of the national security scheme, the technical capabilities in place in the Ministry of Defense, and a study of the international context. In the final analysis it emerged that the Ministry of Defense had the greatest capacity for handling these issues in an efficient and coordinated manner.

Accordingly, over the last two years, the Ministry of Defense has worked to position the issue of cybersecurity and cyberdefense on the national agenda.

While Colombia does not yet have cyber incident response agencies, it does have capabilities and expertise that have allowed it to be a part of commissions that have assisted other governments in the region (Panama, Dominican Republic, and Mexico) in planning their respective Computer Security Incident Response Teams (CSIRTs).

Finally, it is noteworthy that the issue of cybersecurity and cyberdefense was included in the 2010-2014 National Development Plan "Prosperity for All," as part of the *Plan Vive Digital* [Live Digital Plan] spearheaded by the Ministry of Information and Communication Technologies, the purpose of which is to encourage widespread Internet use with the aim of taking a leap toward democratic prosperity.

### B. International framework

The principal international instruments on cybersecurity and cyberdefense are:

| INSTRUMENT | SUBJECT MATTER |
|---|---|
| Council of Europe Convention on Cybercrime[14] (CCC), also known as the Budapest Convention on Cybercrime<br><br>Adopted in November 2001; in force as of July 1, 2004. | The main objective of the Convention is the adoption of legislation to facilitate the prevention of criminal conduct as well as to contribute efficient tools in the area of criminal law with which to detect, investigate, and punish unlawful behavior.<br><br>The Convention, together with its additional protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, is the only binding international instrument in this area. The Council considers that cybercrime requires a common criminal policy aimed at the protection of society against cybercrime[15] , in particular by adopting appropriate legislation and strengthening international cooperation. It should be noted that although the CCC originated in the European region, it is an instrument that is open to all countries for accession. |

14. Any crime committed using a computer or a computer service (Ministry of Defense of Colombia).

15. Hypothetical or imaginary environment or space of those immersed in the world of electronics, informatics, and cybernetics. (Free translation of the definition coined by the Academy of the Spanish Language)

| INSTRUMENT | SUBJECT MATTER |
|---|---|
| OAS General Assembly resolution AG/RES. 2004 (XXXIV-O/04). | Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity.<br><br>The Strategy envisages three lines of action:<br><br>• Creation of a Hemispheric Network of Computer Security Incident Response Teams (CSIRTs).[16] This task was assigned to the Inter-American Committee against Terrorism (CICTE).<br><br>• Identification and adoption of technical standards for a secure Internet architecture. This task is being carried out by the Inter-American Telecommunication Commission (CITEL).<br><br>• Adoption and/or adaptation of the legal tools necessary to protect Internet users and information networks from criminals and organized crime groups that exploit these systems. This was assigned to the Meeting of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA). |
| Andean Community Decision 587 adopted on July 10, 2004 | Which establishes the guidelines of the Andean Common External Security Policy. Among others, the objectives of that policy are to prevent, combat, and eliminate new security threats and, as appropriate, their interactions, through cooperation and coordinated measures to confront the challenges that those threats pose to the Andean Community. |
| Consensus on cybersecurity[17] of the International Telecommunication Union (ITU), in the framework of the United Nations, in pursuance of the Tunis Agenda for the Information Society (2005). | Aimed at promoting consideration of pertinent international concepts designed to strengthen the security of worldwide information and telecommunication systems. |
| UN General Assembly resolution | The General Assembly calls upon member states to promote further at |

16 Por sus siglas en inglés: Visit www.first.org.

17 The collective and coordinated operational response of a country, which recognizes information as a critical asset for safeguarding its governance and, therefore, develops and ensures standards and systematic practices geared toward individuals, technologies, processes, and regulatory and enforcement aspects.

| INSTRUMENT | SUBJECT MATTER |
|---|---|
| 64/25 "Developments in the field of information and telecommunications in the context of international security" (2009) | multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information<br><br>This resolution continues the Assembly's follow-up together with resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007 and 63/37 of 2 December 2008. |

Table 4: International legal framework on cybersecurity

There are Computer Security Incident Response Teams (CSIRT) in place in 13 countries in the region: Argentina (ArCERT), The Bahamas (Royal Bahamas Police), Bolivia (CRISIS), Brazil (CTIR-GOV), Canada (CCIRC), Chile (CORE/ Min. Interior), Guatemala (CSIRT- GT), Paraguay (CSIRT-Py), Peru (PerCERT), Suriname (SurCSIRT), United States (USCERT), Uruguay (CERTUy), and Venezuela (VenCERT).[18] According to the Carnegie Mellon University database (CERT- CC, www.cert.org/csirts/national/contact.html#), there are 55 national CERTS worldwide.

In addition, as the following table shows, different parts of the world have seen the implementation of cybersecurity and cyberdefense policies, the incorporation of new technological capacities, and the activation of agencies to perform these functions:

| COUNTRY | GOVERNMENT MEASURES |
|---|---|
| GERMANY | The German government launched its Strategy on Cybersecurity in February 2011. In April 2011, the Ministry of the Interior launched the National Cyberdefense Center. |
| AUSTRALIA | Opened the Cyber Security Operations Centre to coordinate government measures steps to deal with incidents in cyberspace. |
| CANADA | Public Safety Canada implemented the Canadian Cyber Incident Response Centre (CCIRC) and in October 2010 adopted Canada's Cyber Security Strategy. |

18. CICTE/OAS

| COUNTRY | GOVERNMENT MEASURES |
|---|---|
| UNITED STATES | Established the unified Cyber Command, which reports to the National Security Agency (NSA), DHS: National Cyber Security Division, US-CERT: United States Computer Emergency Readiness Team and the White House Cyber Security Office. The International Strategy for Cyberspace was adopted in May 2011. |
| ESTONIA | In 2008 it created, together with other European countries, NATO, and United States, the Cooperative Cyber Defense Center of Excellence. 2008 also saw the adoption of the Cyber Security Strategy. |
| FRANCE | Created the French Network and Information Security Agency (FNISA), which monitors governmental and private computer networks in order to protect them from cyber attack. An Information Systems Defense and Security Strategy was adopted in February 2011. |

Table 5: Cyberdefense measures adopted at the international level

## III. ANALYSIS

### A. Core Problem

The agencies involved in the preparation of this document have concluded that the current capacity of the State to deal with cyber threats has major weaknesses. Despite the existence of governmental, private, and civil-society initiatives to counter the impact of such threats, an appropriate, coordinated, interagency approach is missing.

At present, Colombia is one of a number of countries that do not have a national cybersecurity and cyberdefense strategy that includes an organizational system and a legal and institutional framework strong enough to confront the latest cybersecurity challenges. Unlike the majority of Latin American countries, Columbia has not yet implemented a national CSIRT or CERT.[19]

19. Computer Emergency Response Team (CERT), equivalent to a CSIRT but registered with Carnegie Mellon University.

The increasing number of Internet users, as well as the strong dependence of Colombia's critical infrastructure on electronic media and the considerable rise in the number of cybersecurity incidents and crimes have highlighted the country's high vulnerability to cyber threats, such as use of the Internet for terrorist purposes, sabotage of public services, espionage, and theft, among others.

## B. Effects of the core problem

The main effects of the above problem are an increase in cybercrime and the risk of unauthorized access to information, impairment of the normal operation and continuity of services, and ongoing impunity in tackling offenses of this type.

There are three (3) main problem areas:

### 1. Cybersecurity and cyberdefense initiatives and operations are not adequately coordinated

Although a number of institutional efforts exist (in both the private and the public sector), the study has found that no agencies have been established at the national level to coordinate and implement cybersecurity and cyberdefense operations. Accordingly, it has not been possible to establish enough adequate mechanisms to curb cyber attacks and protect state interests in cyberspace. Efforts to raise awareness and generate a culture of prevention and safety on the issue of cybersecurity in the public and private sectors as well as civil society have been weak.

### 2. Insufficient availability and coverage of specialized training in cybersecurity and cyberdefense

Expertise in the areas of cybersecurity and cyberdefense in both the public and the private sector is limited. Although a number of higher education institutions in the country offer specialty courses in computer security and computer law, the study noted that the availability of specialized academic programs in these areas is low. Accordingly, a significant number of students who embark on some form of

education in the area of information security do so by enrolling in programs offered by foreign institutions that do not address the Colombian reality in any depth.

The training and education offered to public- and private-sector employees to respond as the first line of defense to cybercrime is deficient. Very often, the chain of custody of digital evidence is lost, hampering forensic investigations. Furthermore, there are a limited number of training programs available for agencies that serve as judicial police in this area.

**3. Weak regulation and legislation on information and data protection.**

In spite of the existence of laws and regulations on information security, shortcomings persist that impede a timely response to cyber incidents and offenses.

The Colombian Congress recently passed the Intelligence and Counterintelligence Law, which introduces monitoring and oversight mechanisms for these activities. However, this law needs to be made much more specific in terms of scope and operability, so that cybersecurity and cyberdefense can be adequately addressed.

In terms of international standards, one of the instruments that would enable the country to draw level with the international community is the Council of Europe's Convention on Cybercrime, under which it would have to meet certain requirements, such as the establishment of judicial cooperation mechanisms, including extradition, points of contact available on a twenty-four hour, seven-day-a-week basis to facilitate investigation, and log-keeping[20] by ISPs,[21] for the requisite amount of time.

In specific areas, such as ISP regulation, significant progress was made in terms of standards toward the end of 2009. The obligation was introduced for ISPs to

---

20. A log is an official record of events over a particular period of time. For computer security professionals a log serves to keep a record of data or information as to the who, what, when, where, and why with regard to an event involving a particular device or an application.

21. Internet service providers (Currently in Colombia these entities also provide telephony and television services, thus becoming providers of integrated telecommunications services.)

implement security models in keeping with the particular features and needs of their networks, with the aim of helping to enhance the security of their access networks, complying with the rules on data confidentiality and integrity, as well as availability of network elements, information, services and applications, in addition to mechanisms for authentication, access and non-repudiation, and obligations in the area of in the area of communications inviolability and information security. . It was found, however, with regard to ISP network security, for example, that logs are not stored for a sufficient length of time, so that, at a given point, they can be used as evidence or contribute to cybercrime investigations.

## IV. OBJECTIVES

### A. Overarching Objective

**To strengthen the capabilities the state to confront threats that undermine its security and defense in cyberspace (cybersecurity and cyberdefense), creating the necessary environment and conditions to provide protection therein.**

This will require the involvement of all government sectors and institutions with responsibilities in the area of cybersecurity and cyberdefense, creating an environment of participation in which all stakeholders act with a common purpose under consensualized strategies and coordinated efforts. It is also vital to inform the public and raise awareness about all aspects of information security; strengthen levels of international cooperation and partnership in areas of cybersecurity and cyberdefense; support investigations of computer attacks, and protect the public from the consequences of those attacks.

### B. Specific objectives

1. **To implement appropriate bodies to prevent, provide assistance, control, produce recommendations, and issue rules on cyber incidents or emergencies, in order to confront threats and risks to national cybersecurity and cyberdefense**.

Through this objective, agencies will be established with the necessary technical and operating capacity to ensure the country's cybersecurity and cyberdefense. To that end, the national government will need to create the following bodies:


Graph 5: Coordination Model
Source: Ministry of Defense

**a.** An Intersectoral Committee charged with devising a strategic vision for information management and with introducing policy guidelines for technology infrastructure management (hardware, software, and communications), public information, and cybersecurity and cyberdefense. This committee would be chaired by the President of the Republic and its members would include, as a minimum, the Chief Advisor on National Security, the Minister of Defense, the Minister of Information and Communication Technologies, the Director of the Department of Security Administration (DAS) or the entity serving as such, the Director of National Planning, and the Coordinator of ColCERT.

Depending on the topics to be addressed, the Committee would also have the possibility to invite other national actors representing academia and the private sector, as well as international experts and representatives of other state institutions.

**b.** Colombia's Cyber Emergency Response Team (ColCERT) will be the agency that coordinates cybersecurity and cyberdefense nationwide. It will provide assistance to and work in partnership with other national bodies, including the Police Cyber Center (CCP) and the Joint Cyber Command (CCOC).

ColCERT will be a Ministry of Defense working group composed of civilian officials, military personnel and representatives of other entities. It will receive guidelines from the Intersectoral Committee.

ColCERT's central objective and mission will be to coordinate the necessary measures to protect the Colombian state's critical infrastructure against cyber emergencies that threaten or compromise national defense and security.

ColCERT will have the following specific objectives:

- To coordinate, together with the Intersectoral Committee, the development and promotion of policies, procedures, recommendations, protocols, and guidelines on cybersecurity and cyberdefense in concert with the relevant stakeholders, as well as ensuring their implementation and compliance.
- To promote local/sectoral capacity building, as well as the creation of sectoral CSIRTs for the operational handling of cybersecurity incidents affecting the country's critical infrastructure, the private sector, and civil society

- To coordinate and advise CSIRTs and other entities in the public and private sectors, as well as civil society, on computer incident response.
- To offer, on demand, prevention services against cyber threats, responses to computer incidents,[22] as well as information, awareness-building, and training to all entities.
- To coordinate the implementation of public-private initiatives and policies on awareness raising and specialized skills development in the areas of cybersecurity and cyberdefense.
- To provide assistance to government security and investigation agencies in prevention and investigation of crimes involving information and communication technologies.
- To foster a knowledge management system in the area of cybersecurity and cyberdefense designed to improve the services rendered by ColCERT.
- To provide the CCP and CCOC with computer intelligence whenever necessary.
- To act as international point of contact with its counterparts in other countries, and with international agencies involved in this issue.

ColCERT is due to start operating in the second half of 2011 within the following the relational scheme:

22. An unwanted or unexpected event that occurs in cyberspace, which, in different circumstances, can harm individuals and affect or cause losses to processes and businesses

**ColCERT Relational Scheme**


Graph 6: ColCERT Relational Scheme
Source: Ministry of Defense

ColCERT will also lead and implement the National Network of CSIRTS and Investigation Agencies. The Network will comprise sectoral CSIRTs and state investigation bodies, and its purpose will be to facilitate and strengthen cooperation and support ties within the country with a view to resolving cybersecurity incidents, through a highly secure platform.

**c.** The Armed Forces Joint Cyber Command (CCOC) will be headed by the General Command of the Armed Forces, who will have the authority to delegate his functions within the Armed Forces subject to the areas of expertise that exist in the sector. It will prevent and counter all cyber threats or attacks that affect the country's assets and interests.

The CCOC will have the following general functions:

- To strengthen the technical and operational capabilities of the country in order to enable it to confront computer threats and cyber attacks through implementation of protection measures at both the hardware and software level, as well as introduction of cyberdefense protocols.
- To protect critical infrastructure and reduce the computer risks to the country's strategic information, as well as strengthen protection for the computer systems of Colombia's security forces.
- To develop neutralization and response capabilities for dealing with computer incidents and attacks against the country's security and defense.

The CCOC will follow national guidelines and work in coordination with ColCERT.

**d.** The Police Cyber Center (CCP) will be in charge of cybersecurity in Colombian territory, offering information, assistance, and protection against cybercrime. Its activities will include prevention, assistance, investigation, and prosecution of computer crime in the country, as well as providing information about vulnerabilities to cyber attack on its website. It will receive and heed the national cybersecurity guidelines and work in coordination with ColCERT.

The CCP will consist of a team appointed by the national police, which will be in charge of the operational response to cybercrime. The operational structure of the CCP will comprise the Virtual Immediate Assistance Command (CAI Virtual), a prevention group, an incident management

group, and an investigation group. The task of CAI Virtual will be to receive information and reports of cybercrimes, and to classify the criminal conduct found. It may also receive requests for talks, training courses, or visits to raise awareness about security issues as it will be in charge of cybercrime prevention and awareness building, which will always be carried out in coordination with ColCERT.

The CCP will investigate cybercrime and provide support in prosecuting cases classified as computer crimes.

In general terms, its functions will be as follows:

- To protect the citizenry from cyber threats/crimes.
- To respond at the operational level to cybercrime, carrying out coordinated efforts in the areas of prevention, assistance, investigation, and support for prosecution of computer crime in the country.
- To provide advisory services on vulnerabilities and threats in computer systems.
- To inform the public to enable preventive steps against the loss of availability, integrity, and/or confidentiality of information.
- To provide assistance and investigate, in coordination with ColCERT, cyber vulnerabilities, threats and incidents that undermine the country's critical computer infrastructure.
- To foster awareness of cybersecurity policies in partnership with stakeholders.

CCP is due to commence operations in 2011.

**2. Provide specialized training in information security and broaden lines of investigation in cybersecurity and cyberdefense.**

This objective will make it possible to generate -and strengthen existing- capacities in the area of cybersecurity, so as to be able to deal with threats that undermine the proposed aims.

At first, training will be provided to staff directly involved in tackling and managing cyber incidents. This training will gradually be extended to all other government agencies. As part of its training plans, ColCERT, with support provided by the OAS Inter-American Committee against Terrorism (CICTE) and others, will carry out a training program for all other civil servants, in addition to implementing awareness raising programs for the general public. Similarly, the Ministry of Defense will endeavor to phase in theoretical and practical courses on information security, cybersecurity, and cyberdefense at officer and NCO training schools.

In the same way, the CCP will seek the collaboration of programs that support the implementation of the accusatory oral criminal justice system, such as the International Criminal Investigative Training Assistance Program (ICITAP), ATA, OPDAT, together with national agencies, such as the School of Criminal Investigation, Criminalistics and Forensic Sciences of the Office of the Attorney General and the Rodrigo Lara Bonilla Judiciary School, among others, in order to introduce legal training programs on computer security for judicial police, prosecutors, and judges.

**3. Strengthen the cybersecurity and cyberdefense laws, bolster international cooperation, and move toward accession by Colombia of the various international instruments in this area**

The purpose of this objective is to develop the necessary legal tools to ensure effective and efficient prevention, investigation, and prosecution of cybercrime.

Thus, moves will be made toward the enactment of the necessary legal framework to comply with international treaties in this regard as they are adopted into the constitutional body of laws. At the same time, efforts will be made to introduce the necessary regulations to implement the country's laws. The institutions responsible for cybersecurity and cyberdefense should seek and evaluate their participation in different international cooperation networks and mechanisms (Council of Europe, OAS, and FIRST), with a view to preparing the country to tackle the increasing cybersecurity challenges that exist on the international plane, as well as to respond more efficiently to cybersecurity incidents and offenses.

Colombia will face the challenge of positioning itself as a regional leader in the area of cybersecurity through exchange of good practices, expertise, and experience, giving particular attention to promoting the country's experience in the cybersecurity and cyberdefense policy development process. To that end, decision-makers and experts on the subject will have to attend international conferences, seminars, and specialized meetings to discuss cybersecurity issues.

In order to achieve all of the foregoing, ColCERT and the CCP will have to combine their initiatives with those of the private sector and civil society.

# V. PLAN OF ACTION

| # A | Acción concreta | Información del Responsable de la ejecución | | Fecha de inicio | Fecha de finalización |
|---|---|---|---|---|---|
| | | Entidad | Dependencia | | |
| | **Implementar la Institucionalidad Adecuada:** | | | | |
| 1 | Aprobar los lineamientos de Política para el desarrollo e impulso de la estrategia de ciberseguridad y la ciberdefensa, presentados en este documento. | Departamento Nacional de Planeación | Subdirección General | 14/07/2011 | 14/07/2011 |
| 2 | Solicitar al Ministerio de Defensa Nacional y al Ministerio de Tecnologías de la Información y las Comunicaciones adoptar el mecanismo de coordinación intersectorial más adecuado para emitir los lineamientos rectores del colCERT. En caso de no existir uno, se solicita su creación. | Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y las Comunicaciones | Despacho de Ministro de Defensa Nacional / Despacho de Ministro de Tecnologías de la Información y las Comunicaciones | 14/07/2011 | 31/12/2012 |
| 3 | Solicitar al Ministerio de Defensa Nacional crear el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT. | Ministerio de Defensa Nacional | Despacho de Ministro de Defensa Nacional | 14/07/2011 | 31/12/2011 |
| 4 | Solicitar al Ministerio de Defensa Nacional que una vez creado el colCERT, emita los modelos de seguridad en el ciberespacio que minimicen el nivel de riesgo al que las entidades están expuestas. | Ministerio de Defensa Nacional | Despacho de Ministro de Defensa Nacional | 14/07/2011 | 30/06/2012 |
| 5 | Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones y a la Comisión de Regulación de Comunicaciones realizar el acompañamiento al Ministerio de Defensa Nacional en las actividades que se consideren pertinentes para la conformación y el desarrollo de las actividades del colCERT. | Ministerio del Tecnologías de Información y las Comunicaciones, Comisión de Regulación de las Comunicaciones | Despacho del Ministro de Tecnologías de la Información y las Comunicaciones, Director Ejecutivo de la Comisión de Comunicaciones | 14/07/2011 | 31/12/2015 |
| 6 | Solicitar al Ministerio del Interior y de Justicia, al Ministerio del Tecnologías de Información y las Comunicaciones, y al Departamento Administrativo de Seguridad o quien haga sus veces, destinar recurso humano con conocimientos técnicos y/o jurídicos en el tema de seguridad de la información y ciberseguridad, para apoyar la ejecución de actividades del colCERT. | Ministerio del Interior y Justicia, Ministerio del Tecnologías de Información y las Comunicaciones, DAS o quien haga sus veces | Despacho del Ministro de Tecnologías de la Información y las Comunicaciones / Dirección General Departamento Administrativo de Seguridad | 14/07/2011 | 31/12/2012 |
| 7 | Solicitar al Ministerio de Defensa Nacional crear el Centro Cibernético Policial – CCP. | Ministerio de Defensa Nacional | Despacho de Ministro de Defensa Nacional | 14/07/2011 | 31/12/2011 |
| 8 | Solicitar al Ministerio de Defensa Nacional crear el Comando Conjunto Cibernético – CCOC. | Ministerio de Defensa Nacional | Despacho de Ministro de Defensa Nacional | 14/07/2011 | 31/12/2011 |
| 9 | Solicitar al Ministerio de Defensa Nacional realizar en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones estudios en seguridad de la información, así como la identificación de la infraestructura crítica nacional. | Ministerio de Defensa Nacional | Despacho de Ministro de Defensa Nacional | 14/07/2011 | 31/12/2012 |
| 10 | Solicitar al Ministerio de las Tecnologías de la Información y las Comunicaciones emitir un documento con las directrices en temas de seguridad de la información basado en estándares internacionales, que deberán ser implementadas por las entidades del sector público. | Ministerio de Tecnologías de la Información y Comunicaciones | Despacho de Ministro de Tecnologías de la Información y las Comunicaciones | 14/07/2011 | 31/12/2013 |

| # A | Acción concreta | Información del Responsable de la ejecución | | Fecha de inicio | Fecha de finalización |
|---|---|---|---|---|---|
| | | Entidad | Dependencia | | |
| 11 | Solicitar a la Comisión de Regulación de Comunicaciones realizar un análisis regulatorio acerca de los aspectos técnicos que deben cumplir los proveedores de redes y servicios de telecomunicaciones para garantizar los principios de confidencialidad de datos, integridad de datos y disponibilidad, así como las medidas para autenticación y acceso de los usuarios a la red y el no repudio de las comunicaciones y, en caso de ser requerido a partir de tal análisis, llevar a cabo los ajustes a que haya lugar frente al marco regulatorio vigente. | Comisión de Regulación de las Comunicaciones | Director Ejecutivo de la Comisión de Comunicaciones | 14/07/2011 | 31/12/2015 |
| **Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberseguridad y ciberdefensa:** | | | | | |
| 12 | Solicitar al Ministerio de las Tecnologías de la Información y las Comunicaciones, facilitar los canales institucionales para que el colCERT pueda realizar la sensibilización y concienciación en temas de seguridad cibernética. | Ministerio de Tecnologías de la Información y las Comunicaciones | Despacho de Ministro de Tecnologías de la Información y las Comunicaciones | 14/07/2011 | 31/12/2012 |
| 13 | Solicitar al Ministerio de Defensa Nacional en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones, diseñar las campañas de sensibilización y concienciación en temas de seguridad cibernética. | Ministerio de Defensa Nacional | Despacho de Ministro de Defensa Nacional | 14/07/2011 | 31/12/2012 |
| 14 | Solicitar al Ministerio de Defensa Nacional implementar gradualmente asignaturas en seguridad de la información, ciberdefensa y ciberseguridad (teórico-prácticas), en las escuelas de formación y de capacitación de oficiales y suboficiales. | Ministerio de Defensa Nacional | Despacho de Ministro de Defensa Nacional | 14/07/2011 | 31/12/2015 |
| 15 | Solicitar al Ministerio de Defensa Nacional adelantar un plan de capacitación en temas de seguridad de la información para los funcionarios del Estado, con el apoyo de organismos internacionales. | Ministerio de Defensa Nacional | Despacho de Ministro de Defensa Nacional | 14/07/2011 | 31/12/2015 |
| 16 | Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones, al Ministerio de Defensa Nacional y al Departamento Administrativo de Seguridad o a quien haga sus veces, diseñar e implementar planes de capacitación en lo referente a seguridad informática, investigación y judicialización de delitos informáticos, para policía judicial. | Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional, DAS o quien haga sus veces | Despacho del Ministro de Tecnologías de la Información y las Comunicaciones, Despacho del Ministro de Defensa Nacional, Dirección General DAS | 14/07/2011 | 31/12/2015 |
| 17 | Sugerir a la Fiscalía General de la Nación en coordinación con el Consejo Superior de la Judicatura diseñar e implementar planes de capacitación sobre temas de investigación y judicialización de delitos informáticos, para policía judicial, jueces y fiscales. | Fiscalía General de la Nación | Coordinador Nacional de Delitos Informaticos | 14/07/2011 | 31/12/2014 |
| 18 | Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA, para la generación de un plan de capacitación para el sector privado en temas de ciberseguridad y de seguridad de la información. | Ministerio de Tecnologías de la Información y Comunicaciones | Despacho de Ministro de Tecnologías de la Información y las Comunicaciones | 14/07/2011 | 31/12/2013 |

| # A | Acción concreta | Información del Responsable de la ejecución | | Fecha de inicio | Fecha de finalización |
|---|---|---|---|---|---|
| | | Entidad | Dependencia | | |
| **Fortalecer la legislación y la cooperación internacional en materia de ciberseguridad y ciberdefensa:** | | | | | |
| 19 | Solicitar al Ministerio del Interior y de Justicia realizar en coordinación con el el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de Información y Comunicaciones, un documento en el que se analice la normatividad actual y se propongan las modificaciones necesarias en materia de seguridad de la información y protección de datos, para prevenir el ciberdelito, identificando las dificultades de interpretación y aplicación. | Ministerio del Interior y Justicia | Despacho de Ministro del Interior y Justicia | 14/07/2011 | 31/12/2013 |
| 20 | Solicitar al Ministerio del Interior y Justicia, en coordinación con el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones, con base en el análisis realizado, adelantar las iniciativas tendientes a expedir o reformar las leyes que sean necesarias así como reglamentar aquellas a que haya lugar, en aras de garantizar el marco normativo adecuado para la ciberseguridad, la ciberdefensa y la seguridad de la información. | Ministerio del Interior y Justicia | Despacho de Ministro del Interior y Justicia | 14/07/2011 | 31/12/2013 |
| 21 | Solicitar al Ministerio de Relaciones Exteriores apoyar al colCERT, en materia de cooperación internacional, en los temas de ciberseguridad, ciberdefensa y seguridad informática, en los que se incluya la designación del colCERT como punto de contacto internacional en temas referentes a la ciberseguridad y la ciberdefensa. | Ministerio de Relaciones Exteriores | Despacho de Ministra de Relaciones Exteriores | 14/07/2011 | 31/12/2012 |
| 22 | Solicitar al Ministerio de Relaciones Exteriores, estudiar la viabilidad y conveniencia para Colombia de adherir a los principales instrumentos internacionales en materia de seguridad de la información y protección de datos, con el directo apoyo del Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones. En caso de que el estudio produzca una recomendación positiva, iniciar los trámites de adhesión al instrumento que corresponda. | Ministerio de Relaciones Exteriores | Despacho de Ministra de Relaciones Exteriores | 14/07/2011 | 31/12/2012 |
| | | Ministerio de Relaciones Exteriores | Dirección de Asuntos Políticos Multilaterales | 14/07/2011 | 31/12/2012 |

[1] Las Leyes se consideraran implementadas con la presentación del proyecto.

## VI. FINANCING

The cost of implementing the cybersecurity and cyberdefense guidelines that ColCERT will issue for public-sector entities will also be covered by the budget allocated to each entity.

The initial implementation of ColCERT, the CCP, and the CCOC in the Ministry of Defense will entail the following appropriations from the Ministry:

| 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|
| $ 1,428,444,328 | $ 5,400,000,000 | $ 5,000,000,000 | $ 4,600,000,000 |

This budget also covers ColCERT operating with a staff of six (6) officials from the Ministry of Defense and other public-sector entities.[23] Moving forward, ColCERT, with the endorsement of the cybersecurity intersectoral coordination mechanism adopted, may consider it necessary to increase the size of the group, which would require a revision of the budget included herein and the support provided by each entity.

It is important to point out that additional funds will be allocated for 2011 in order to assist the General Command of the Armed Forces in implementing the CCOC.

In 2011, the funding for the three centers will be provided by the operating budget. From 2012 onward, the funding will come from investment in three projects that have already been registered in the Investment Projects Bank.

## VII. RECOMMENDATIONS

The Ministry of Defense, the Ministry of Information and Communication Technologies, the Ministry of the Interior and Justice, the Ministry of Foreign Affairs, the National Planning

23. The staff from other public-sector entities will be assigned to the group under a temporary commission.

Department, and the Department of Security Administration make the following recommendations to the National Council on Economic and Social Policy (CONPES):

**Implement the appropriate institutional framework**:

1. Approve the policy guidelines presented in this report for the development and implementation of the cybersecurity and cyberdefense strategy.

2. Request the Ministry of Defense and the Ministry of Information and Communication Technologies to adopt the most suitable intersectoral coordination mechanism for issuing the ColCERT guidelines. Should none exist, it is requested that one be created.

3. Request the Ministry of Defense to create the Colombian Computer Emergency Response Team (ColCERT).

4. Request the Ministry of Defense, once ColCERT has been established, to issue cybersecurity guidelines that minimize the level of risk to which entities are exposed.

5. Request the Ministry of Information and Communication Technologies and the Communications Regulation Commission to work with the Ministry of Defense on such activities as are deemed pertinent for establishing and implementing ColCERT's activities.

6. Request the Ministry of the Interior and Justice, the Ministry of Information and Communication Technologies, and the Department of Security Administration or the entity serving as such, to assign human resources with technical and/or legal expertise in the area of information security and cybersecurity in order to assist in the implementation of ColCERT's activities.

7. Request the Ministry of Defense to create the Police Cyber Center (CCP).

8. Request the Ministry of Defense to create the Joint Cyber Command (CCOC).

9. Request the Ministry of Defense, in coordination with the Ministry of Information and Communication Technologies, to carry out information security studies and identify the country's critical infrastructure.

10. Request the Ministry of Information and Communication Technologies to issue a document containing information security guidelines based on international standards, which public-sector entities would be required to implement.

11. Request the Communications Regulation Commission to carry out a review of regulations on technical aspects to be met by telecommunications services and network providers in order to conform to the principles of data confidentiality, data integrity, and availability, as well as authentication and user network access mechanisms, and non-repudiation of communications; and request the Commission, if necessary, based on the review, to implement the appropriate adjustments to the regulatory framework in force.

**Provide specialized training in information security and broaden lines of investigation in cybersecurity and cyberdefense.**

12. Request the Ministry of Information and Communication Technologies, to facilitate institutional channels to enable ColCERT to carry out awareness raising on cybersecurity.

13. Request the Ministry of Defense, in coordination with the Ministry of Information and Communication Technologies, to design cybersecurity awareness raising campaigns.

14. Request the Ministry of Defense to phase in courses on information security, cybersecurity and cyberdefense (theory-practical) at officer and NCO training schools.

15. Request the Ministry of Defense to carry out a civil-servant training program on information security and cybersecurity, with the support of international agencies

16. Request the Ministry of Information and Communication Technologies, the Ministry of Defense, and the Department of Security Administration or the entity serving as such, to design and implement training programs for judicial police on information security and on computer crime investigation and prosecution.

17. Suggest to the Office of the Attorney General of the Nation that, in coordination with the Superior Council of the Judicature, it design and implement training programs on computer crime investigation and prosecution for judicial police, judges, and prosecutors.

18. Request the Ministry of Information and Communication Technologies to make the necessary arrangements with the Ministry of Education and the SENA to develop a cybersecurity and information security training program for the private sector.

**Strengthen laws and international cooperation on cybersecurity and cyberdefense:**

19. Request the Ministry of the Interior and Justice to prepare, in coordination with the Ministry of Defense and the Ministry of Information and Communication Technologies, a document that reviews the standards in place and proposes the necessary modifications as regards information security and data protection, in order to prevent cybercrime, as well as identifying difficulties in terms of interpretation and enforcement.

20. Request the Ministry of the Interior and Justice, in coordination with the Ministry of Defense and the Ministry of Information and Communication Technologies, to implement, based on the review carried out, initiatives to enact or reform the necessary laws, and, as appropriate, adopt implementing regulations for laws, in a bid to ensure an adequate legal framework for cybersecurity, cyberdefense, and information security.

21. Request the Ministry of Foreign Affairs, with regard to international cooperation in the areas of cybersecurity, cyberdefense, and information security, to support ColCERT in those instances for which it has been designated the international point of contact for cybersecurity and cyberdefense.

22. Request the Ministry of Foreign Affairs to examine the feasibility and advisability of Colombia's accession to the principal international instruments on information security and data protection, with direct assistance from the Ministry of Defense and the Ministry of Information and Communication Technologies. Should the study result in a positive recommendation, initiate the formalities for accession to the appropriate instrument or instruments.

## VIII. SELECT BIBLIOGRAPHY

usCERT – Estados Unidos: http://www.us-cert.gov

Carnegie Mellon University/CERT Coordination Center: http://www.cert.org/csirts/

U.S. National Strategy To Secure Cyberspace http://www.whitehouse.gov/pcipb/

Forum Of Incident Response Security Teams (FIRST): http://www.first.org

Inter-American Committee against Terrorism (CICTE), Organization of American States: http://www.cicte.oas.org

Inter-American Cooperation Portal on Cybercrime: http://www.oas.org/juridico/english/cyber.htm

ENISA Setting-up Guide. A Step-by-Step Approach on How to Set up a CSIRT.

## IX. GLOSSARY OF TERMS

BotNet: The name given to a network of computers that combines their resources to perform a common task and shares the workload among all the computers (FireEye – Arbornet).

CERT: Computer Emergency Response Team. (Carnegie-Mellon University)

Computer risk: The possibility that a concrete threat could exploit a vulnerability in order to cause a loss or harm to an information asset. (ISO Guide 73:2002)

Convergence: Coordinated evolution of formerly discrete networks towards uniformity in support of services and applications. (Rec. ITU-T Q.1761, 3.1)

Critical infrastructure: The array of computers, computer systems, and telecommunications, data, and information networks, whose destruction or interference could weaken or impact on the security of a country's economy, public health, or both. (CRC resolution 2258 of 2009)

CSIRT: Computer Security Incident Response Team. (http:// www.first.org)

Cyber attack: An organized and/or premeditated act by one or more persons to harm or cause problems to a computer system via cyberspace. (Ministry of Defense of Colombia)

Cybercrime: An illegal or abusive activity connected with computers or communications networks in which a computer is used as a tool to commit the offense or the target of the offense is a computer system (or its data). (Ministry of Defense of Colombia)

Cyberdefense: The state's capacity to prevent and counter any cyber threat or incident that undermines national sovereignty.

Cyber incident: Any real or suspected adverse event in relation to the security of computer systems or computer networks: http://www.cert.org/csirts/csirt_faq.html CERT/CC.

Cybernetic: Adjective meaning of or relating to cybernetics (e.g., cybernetic organ, cybernetic process). (Translation of the definition coined by the Academy of the Spanish Language)

Cybernetics: The science or discipline that studies automatic communication and control mechanisms or the operating technology of connections in living beings and in machines. (Translation of the definition coined by the Academy of the Spanish Language)

Cybersecurity: The state's capacity to minimize the level of exposure of its citizens to cyber threats or incidents.

Cyberspace: The physical and virtual environment composed of computers, computer systems, computer programs (software), and telecommunications, data, and information networks, in which users interact with each other. (CRC resolution 2258 of 2009).

Cyberterrorism: The convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein. To qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Examples include attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss. (Dorothy Denning, Georgetown University)

Cyber threat: The appearance of a potential or actual situation in which an agent has the capacity to produce a cyber attack against the population, territory, and political organization of the state. (Ministry of Defense of Colombia)

DDoS: Distributed Denial of Service. Ataques Distribuidos de Denegación de Servicio. (http://www.rediris.es)

DOS: Denial of Service. Service not available to a person or process (application) when necessary (availability). (http://www.rediris.es)

Electronic Services (or e-Services): The improvement in the provision of public services to citizens via cyberspace.

ICTs: Information and Communication Technologies Collection of resources, tools, equipment, computer programs, applications, networks, and media that enable the compilation, processing, storage, and transmission of information as voice, data, text, video, and images. (Law 1341/2009 TIC)

IP (Internet Protocol): A numerical label assigned, logically and hierarchically, to the interface (communication/connection element) of a device (normally a computer) within a network that uses the IP protocol. (http://www.iso.org)

ISO: International Organization for Standardization, which has its headquarters in Geneva, Switzerland. A worldwide federation of national standards institutes promoting the development of standardization of goods and services. (http://www.iso.org)

ISO 27001: ISO standard for information security management systems transcribing the second part of BS 7799. It is certifiable. (http://www.iso.org)

ISO 27002: Code of practice for information security management (transcript of ISO 17799). It is not certifiable. (http://www.iso.org)

ISP: Internet service providers. In Colombia these entities also provide telephony and television services, which makes them providers of integrated telecommunications services.

IT: Information technologies.

Logical security: Consists of the application of barriers that guard access to data whereby only authorized persons are allowed access. (http://www.segu-info.com)

Logs: An official record of events over a particular period of time. For computer security professionals, a log serves to keep a record of data or information as to the who, what, when, where, and why with regard to an event that involves a particular device or application.

NAP (Network Access Point) Colombia: The national connection point for ISP networks in Colombia, which ensures that Internet traffic to and from our country only uses local or national channels. (www.nap.com.co)

NTC5411- 1 Information and communication technologies security management. (ICONTEC International publications catalog)

Telecommunications: Any transmission and reception of signs, signals, writing, images and sound, data, or information of any nature by wire, radiofrequency, optical media, or other electromagnetic systems. (MinTIC resolution 202 of 2010).

Threat: Potential security breach. (Rec. UIT-T X.800, 3.3.55)

UNESCO - United Nations Educational, Scientific and Cultural Organization

Zombies: The name given to computers that have been remotely infected by a malicious user with some kind of software that, upon infiltrating the manipulated computer without the consent of the user allows a third party to use it and perform illicit activities over the web. [Instituto Nacional de Tecnologías de la Comunicación, (INTECO) – CERT, Spain].

## ACRONYMS AND ABBREVIATIONS

CCD: Cooperative Cyber Defence Centre of Excellence

CCIT: Colombian Chamber of Informatics and Telecommunications

CCOC: Joint Cyber Command

CCP: Police Cyber Center

CICTE: Inter-American Committee against Terrorism

COINFO: Intersectoral Committee on Information Policy and Management in the Public Administration

ColCERT: Cyber Emergency Response Team of Colombia (Ministry of Defense of Colombia)

CONPES: National Council on Economic and Social Policy

CRC: Communications Regulation Commission

DAS: Department of Security Administration

FIRST: Forum on Incident Response Teams

FBI: Federal Bureau of Investigation

IEC: International Electrotechnical Commission

ISO: International Organization for Standardization

ITU: International Telecommunication Union

MDN: Ministry of Defense.

MinTIC's: Ministry of Information and Communication Technologies

NATO: North Atlantic Treaty Organization

OAS: Organization of American States

UNESCO: United Nations Educational, Scientific and Cultural Organization


National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu