CYBER SECURITY TECHNICAL ASSISTANCE MISSION

CONCLUSIONS AND RECOMMENDATIONS

April 4th, 2014
Bogotá, Colombia

Organization of
American States

The Colombian government approached the Organization of American States (OAS) for support in organizing an International Commission of Experts to evaluate the status of cybersecurity in the country. This reflects the interest of Mr. Juan Manuel Santos Calderon, President of the Republic of Colombia, in making information technology and communications part of an integral plan for development of the country. After visiting Colombian institutions, hearing presentations, and exchanging ideas with relevant actors with responsibility over national cyber security, the international experts prepared a series of recommendations for the Colombian government to take into account. The International Commission of Experts offered their experience in the politics of cyber security, international frameworks, responses to cyber security, investigation, and legislation for cybercrime, cyber defense, and international cooperation. The international experts that participated in this Technical Assistance Mission, are officials of the governments of Canada, Spain, the United States, the UK, the Dominican Republic, Estonia, Israel, the Republic of South Korea, and Uruguay. Similarly, in addition to officials from the OAS, this International Commission was attended by representatives of the Council of Europe (COE), the World Economic Forum (WEF), INTERPOL, the Organization of United Nations (ONU), the Organization for Economic Cooperation and Development (OECD), and the University of Oxford. The recommendations from the experts were drafted in private sessions, guaranteeing an equal and impartial analysis of the needs and paths forward that the Colombian government should consider. Although the OAS organized this International Commission of Experts, this document does not reflect the position or opinion of the international organization.

CONTRIBUTORS

INTERNATIONAL EXPERTS

CLAUDIO PEGUERO
DOMINICAN NATIONAL POLICE
DARKO LOVRIC
WORLD ECONOMIC FORUM
DIRK NONNINGER
UNITED NATIONS COUNTER-TERRORISM EXECUTIVE DIRECTORATE
ELVIRA TEJADA
SPANISH PROSECUTION SERVICE
EREZ KREINER,
ISRAELI NATIONAL CYBER BUREAU
ERWIN DOTZAUER
UNIVERSITY OF OXFORD
GWEN BEAUCHEMIN
PUBLIC SAFETY CANADA
IAN MABBOTT
UK TRADE AND INVESTMENT
LAURENT BERNAT
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
LAURI LUHT
ESTONIAN INFORMATION SYSTEMS AUTHORITY
MANUEL SICILIA SAN JOSÉ
NATIONAL CENTRE FOR CRITICAL
INFRASTRUCTURE PROTECTION (CNPIC) – SPAIN
MARCOS SALT
COUNCIL OF EUROPE

NATHAN DOYEL
U.S. DEPARTMENT OF STATE
ROBERT GORDON
PUBLIC SAFETY CANADA
RODOLFO ORJALES
MEETINGS OF MINISTERS OF JUSTICE OR OTHER
MINISTERS OR ATTORNEYS GENERAL OF THE AMERICAS (REMJA)
SANTIAGO PAZ
E-GOVERNMENT AND INFORMATION SOCIETY OF URUGUAY
YOUNG-JUN KIM
KOREA INTERNET & SECURITY AGENCY

NATIONAL EXPERTS

MINISTRY OF DEFENSE
SONIA JULIANA GARCÍA VARGAS
OSCAR JAVIER ARIAS ARIAS
WILSON PRIETO
CORONEL FREDDY BAUTISTA
MAYOR LUIS ATUESTA
MAYOR ALEX DURAN
TENIENTE JHON GUEVARA
CF. WILLIAM HERNANDEZ
C. MILENA REALPE
M. DIDIER SUAREZ
MAYOR DANIEL UCRÓS
JAIRO BECERRA
GUILLERMO MENDOZA
YANETH YATE HURTADO
WILSON FERNANDO CARVAJAL
JAVIER PABON RIVAS
MANUEL DÍAZ HOYOS
CORONEL MARTHA LILIANA SANCHEZ
CR. JAIRO ANDRÉS CÁSERES
CF. CONSTANZA BERMUDEZ
CF. GERMÁN GARZÓN
TE. ZABALA LOPEZ

TE. PINTO ANDREA
TE. ANDRÉS FELIPE CAMPOS
TC. JAVIER BARRERA

MINISTRY OF ICT
MARÍA ISABEL MEJÍA
JORGE FERNANDO BEJARANO
LUIS ALEJANDRO BECERRA
HUGO SIN TRIANA
ALEJANDRO DELGADO
LUCIA ALEMAÑY
JULIAN DAVID ZULUAGA
CLAUDIA HURTADO

MINISTRY OF JUSTICE AND LAW
AUGUSTO IBAÑEZ
ORLANDO SARMIENTO
PAULA GALLO CAICEDO
MARIA FERNANDA FUENTES

JUDICIAL BRANCH
ALEXANDER DÍAZ

PRIVATE SECTOR AND ACADEMIA
DIEGO ZULUAGA
JEIMY CANO
JOSÉ MONTOYA
MANUEL SANTANDER
ANDRES GALINDO
GONZALO ROMERO
JOSÉ MIGUEL DE LA CALLE
CLAUDIA BUSTAMANTE
MANUEL DÁVILA
BIATRIZ CAICEDO
JUAN DIEGO JIMENEZ
ANDRÉS GUZMAN

ORGANIZATION OF AMERICAN STATES (OAS)

NEIL KLOPFENSTEIN
EXECUTIVE SECRETARY
INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)

PABLO MARTINEZ
SENIOR PROGRAM MANAGER
AND PROGRAMS COORDINATOR, OAS/CICTE

BELISARIO CONTRERAS
CYBER SECURITY PROGRAM MANAGER
OAS/CICTE

BRIAN DITO
CYBER SECURITY ASSISTANT PROGRAM MANAGER
OAS/CICTE SECRETARIAT

1 - STRENGTHENING INSTITUTIONAL CAPACITIES FOR CYBER SECURITY AND CYBER DEFENSE

The recommendations below are focused on the five areas considered the most fundamental. It is recognized that there may be other aspects that are worthy of consideration such as public awareness, skills development, etc.

This document uses the term "cybersecurity" to cover the concepts of "cybersecurity" and "cyberdefense" as defined in CONPES 3701.

The Recommendations below take into account the specific national security challenges faced by Colombia and the critical role played by the Ministry of Defense, and that role must continue. Our recommendations recognize the need to preserve the capacity of the Colombian security agencies.

Challenge 1. Colombia's efforts to address cybersecurity are limited by the lack of a clear overarching vision.

Security is not an end in itself. It is a means supporting higher level objectives.

While CONPES 3701 represents an important step forward, it does not approach the issues at a high level to provide a clear strategic vision. At the present stage, the Government's understanding of the subject matter (e.g. definition of cybersecurity and cyberdefense) and overarching goals seem to be guided by institutional considerations and interests rather than by a clear vision for the country transcending these considerations. Institutional matters are essential to implement a strategic vision, however they only cover one aspect. They should result from the vision rather than the reverse.

Recommendation 1: develop an overarching vision ("the vision") for cybersecurity.

The vision should:

- Clearly formulate the high-level and comprehensive objectives pursued and articulate why they are essential for the nation.
- Clearly distinguish objectives of:
    1. Economic and social prosperity,
    2. Defense of the country (e.g. military, intelligence, etc.), and
    3. Fight against cybercrime.

These 3 objectives are different in nature and should be addressed separately. However, they also overlap in some areas. This overlap should be addressed specifically (e.g. through appropriate coordination mechanisms) rather than drive the whole vision.

- Recognize the need to respect the values established in the Constitution.
- Be led at the highest level of the government. This will ensure that:
    - The vision is understood and followed by everyone within the government, and throughout the economy and society.
    - The above three competing and sometimes contradictory objectives are balanced in the best interest of the nation.
- Encompass international co-operation. The digital environment is inherently global. Most aspects of cybersecurity risk management have an international character.

Challenge 2. The overall cybersecurity approach is not based on risk management.

Security measures are being adopted without resulting from systematic risk assessment and management. The current approach aims to achieve security instead of managing the risks. A risk management approach aims to realize the benefits of the digital environment for economic and social prosperity. As Colombia is going increasingly digital, a security approach (i.e. not based on risk management) will become increasingly unsustainable and costly without effectively protecting the economy and society. This will be particularly the case with respect to critical infrastructure protection.

From an organizational perspective, there are two main issues: 1/ The highest level of government does not have a comprehensive assessment of the overall country-wide cybersecurity risk situation and therefore cannot make risk-based decisions, 2/ Activities at lower levels are not based on risk management.

Recommendation 2: Adopt an overall cybersecurity risk management approach.

- Base the overarching vision on a risk management approach.
- Establish a national risk management programme (including assessment, treatment, selection of security measures, preparedness, recovery), and methodology for all actors to assess and manage cybersecurity risks, including awareness, training, etc.
- Establish a capacity to develop a comprehensive national cybersecurity risk assessment.

Challenge 3. Responsibility is not clearly distributed throughout the government and some institutions have responsibility without authority or resources to act.

The institutional framework is complex and it is not clear who is responsible for what. The impression created is that accountability is vague and coordination complicated without clear mechanisms.
The allocation and planning of resources are not clear and do not result from a comprehensive assessment of the overall country-wide cybersecurity risk situation, covering the 3 objectives identified above.

The absence of an authority responsible for overall coordination leads to a potential duplication of efforts and reduced efficiency. The existing institutional dynamic appears to be driven by resource allocation rather than cybersecurity risk management objectives.

Recommendation 3: establish a clear institutional framework.

This framework should:

- Establish a permanent coordination body ("coordination body") with an overarching government-wide role. This body should report directly to the President.
- Assign to the coordination body:
    - The statutory responsibility and authority to act, including budgetary resources to deliver the vision.
    - The responsibility for leading public policy making to ensure a coherent whole of government approach.
    - The establishment of the above national risk management programme.
- Provide to the coordination body the capacity to develop a comprehensive national cybersecurity risk assessment.

Consideration should be given to locate the national CERT (currently colCERT) within the coordination body. The coordination body must ensure the independence of entities constitutionally mandated to carry out judicial functions.

Challenge 4. The mechanism for comprehensive engagement with all stakeholders (incl. private sector, academia, civil society, international entities) is not mature1

A public-private dialogue has commenced. However, in getting to the next level of maturity for cybersecurity risk management, it should be significantly enhanced and engage all components of the economy and society. All stakeholders are responsible for the management of cybersecurity risks, according to their role. Therefore, the implementation of the vision relies on their full engagement. Involving all stakeholders (public and private) in the development of the vision, policies, and their implementation is essential to maximize their engagement.

Recommendation 4: establish a systematic process to engage all stakeholders in the development of the strategy and its implementation.

- Consult all stakeholders on how to organize the systematic multistakeholder dialogue.
- Establish rules to systematically consult all stakeholders at the early stage of and throughout policy development.
- Building on existing efforts, create forums for all stakeholders to participate in the execution of the vision
- Develop a short, medium and long term plan to progressively reach out to all governmental and non-governmental players.

Challenge 5. The focus of the government regarding the protection of critical infrastructures is limited

Critical infrastructure policy is on the government's agenda and a process has commenced to identify critical infrastructures and associated issues (e.g. related to supply chain). However, a definition of what is critical infrastructure has not yet been developed and therefore what needs to be protected is unknown. Colombia is at the early stage of critical infrastructure policy. Most critical infrastructures are owned and operated by the private sector and should therefore be at the center of the development of the critical infrastructure protection policy. However, it does not seem to currently be the case in the planned critical infrastructure protection policy.

[1] Additional guidance on this topic can be found in recommendations in the "Legal Frameworks" and "International Cooperation" sections.

Recommendation 5. The government should adopt a policy for the protection of critical infrastructure taking into account the personnel, physical, and logical aspects.

- Digital aspects of critical infrastructure protection policy should be part of the vision. The digital (or cyber) aspect of critical infrastructure protection should be a subset of the comprehensive approach to protect critical infrastructure.
- Critical infrastructure policy contributes to both the economic and social prosperity of the country, as well as its defense. Therefore, the coordination body should lead this policy making process to ensure that these sometimes competing objectives are appropriately balanced in the best interest of the country.
- The description of colCERT's role in CONPES 3701 ("colCERT Relational Scheme", graph 6) reflects an appropriate approach to critical infrastructure protection with respect to the implementation of the vision in the area of critical infrastructure protection. However, since critical infrastructure policy overlaps between the objective of economic and social prosperity and defense of the country, this function should be positioned as part of the coordination body (and should not be called a "CERT").

2 - CREATION AND IMPROVEMENT OF CYBER SECURITY LEGAL FRAMEWORKS

1. In accordance with the recommended approach of the Group of Experts on Cyber-Crime-REMJA (OAS), it is suggested that the government of Colombia reform its legislation in line with the Budapest Convention, especially with regard to issues of Criminal Procedural Law. This will also subsequently lead to adherence with the Council of Europe Convention. Additionally, it is recommended that the government reference other successful cyber laws such as the Law 53-07 of the Dominican Republic and the Law 109 passed on September 15, 2009 in Portugal. For the purposes of drafting and defining the criminal offenses, it is recommended that the importance of using technologically neutral language be considered so that offences may be applied to both current and future crimes.

2. Issues pertaining to the investigation and prosecution of cybercrime must be adequately separated from the issues of cyber defense and cyber war, ensuring that police units be specifically in charge of the prevention, investigation and prosecution of cybercrime. This is in addition to timely interagency collaboration.

3. Establish a fast and efficient system to ensure international cooperation in the prevention, investigation and prosecution of cybercrime. Among them, it is specifically recommended that a contact point for the 24/7 Network be available 24 hours a day, 7 days a week. This will ensure the provision of immediate assistance for the purpose of investigations or proceedings related to computer systems and data offenses, or for the collection of electronic evidence of a crime.

4. It is recommended that measures be adopted so that legal professionals conform with Article 12 of the European Convention of Budapest.

5. In all regulations relating to the procedural powers for investigating computer crimes, the need for an appropriate balance between investigative efficiency and the protection of individual rights must be taken into account, especially with regard to privacy and the right to data protection.

6. Given the volatile nature of digital evidence, it requires quick and immediate attention. Therefore, the promotion of measures and procedural powers that enable the preservation of data specified in accordance with the provisions of Article 16 and 17 Budapest Convention are recommended

7. Implement legislation in Colombia to require the retention of traffic data for a minimum term of one year, ensuring the constitutional rights of the country and the international agreements signed by Colombia.

8. The government should request that the main Internet service providers, which host servers for Colombian citizens data, review the mechanisms of cooperation in criminal matters and enable these companies to respond in a timely manner to assistance requests in criminal matters.

9. Recommend the creation of specialized national prosecution units who prepare research and specify the exercise for criminal action in cyber-crime cases and offenses that involve electronic evidence.

10. Organize training courses for judges and prosecutors, which focus on computer crime and on the technical and legal aspects of obtaining digital evidence, remaining mindful of the legality and constitutionality of extracting digital evidence.

11. Promote laws and regulations that outline the obligations for companies that control critical infrastructure, with regard to reporting computer security incidents within a period of 48 hours, under guarantee of confidentiality.

To apply the recommendations outlined above, we understand that it is critical to take into consideration the views of the legal system experts, the Academia and Civil Society representatives.

3 - CREATION OF CYBER SECURITY AND CYBER DEFENSE CAPABILITIES

1. Establish a national civilian cyber security capability including a Computer Incident Response Centre and a national civilian security operations centre within the permanent coordination body as referred to previously. It will take time to establish cyber security maturity and consideration should be given to an transformation program to ensure this takes place in a timely and coordinated manner.

2. Establish channels for two-way information sharing. The computer incident response centre ("the Centre") must receive incident feeds from all constituents (critical infrastructure elements, public and private sector SOCs, and government entities including policy, military and international). The Centre would provide guidance and support to critical infrastructures, including advice on applicable or mandatory cyber security standards. The Centre would inform affected constituents of operational incidents that require action.

3. The Centre, SOCs, and other authorities must establish a robust technical analytic capacity. Analytical tools and training to use them must be acquired to examine trends in the national threat environment, including capabilities in reverse engineering for deep technical work in malware analysis, emerging cyber issues, mobile technology, monitoring of new national broadband infrastructure, big data analytics, process control systems, advanced tool development in visualization and automation, and others.

4. To address cyber security in Colombia, there is a need for adequate human and financial resources to fulfil national cyber security mandates. The government should establish a professional cyber academy to train cyber security professionals and promote accreditation and certification of other cyber education in the country. Similarly, descriptions of cyber jobs and required knowledge, skills and background must be promoted by the coordinating body. Awareness regarding careers in cyber security and cyber agencies to attract and retain talented workers must be disseminated, which includes professional exchanges.

5. The coordinating body needs to ensure that key professional services are certified, like penetration testing, red-blue teaming, and others.

6. Innovation centers must be established where Colombians can pursue cyber security entrepreneurship. Importance must be placed on small and medium enterprises, which are significant sources of innovation.

7. Consideration needs to be given to the financial burden on small and medium enterprises operators, and sectors with few financial resources of developing cyber security capabilities, through tax incentives, grants, or other mechanisms.

8. The coordinating body should be a repository for best cyber security practices in Colombia, including guidance and advice on standards, and frameworks for accreditation, and certification.

4 - INTERNATIONAL AND MULTI-STAKEHOLDER COOPERATION

Information security is a multi-stakeholder issue. Effective work in this area requires deep and sustained cooperation with the private sector (national and international) as well as with foreign governments, international organizations, and academic experts.

The recommendations outlined here should be adopted by the relevant institutions within the Government of Colombia, and should be should include extensive consultation with the private sector.

1. Develop a written strategy for international cooperation that addresses cyber security and cybercrime. The strategy should identify priorities, international partners, and objectives. All government entities concerned with cybercrime and cyber security should be involved in the strategy´s development and the document should be approved at the highest levels of government. The strategy should be integrated into the government's broader foreign policy strategies, planning documents, and resource requests.

2. Expand the role of the Ministry of Foreign Affairs in international cooperation on cyber security. Strengthen the capacity of the Ministry of Foreign Affairs to carry out the necessary international cooperation.

3. Consider the creation of the position of Coordinator for International Cyber Policy, whose main responsibility will be to implement the international cooperation strategy. At the same time, this individual should maintain a strong relationship and establish a feedback loop with domestic policy and decision makers and technical experts, so that all stakeholders have a holistic view of cyber security policy.

4. Work to establish national and international public-private cooperation in the area of cyber security by developing a formal mechanism between government and the private sector that is secure and accessible to exchange information regarding national and international cyber security incidents. This mechanism should allow for two-way information sharing[2] between the government and the private sector and should also include active information sharing regarding cyber security policy and allow for a mutual exchange of ideas between the government and a wider scope of the private sector.

[2] Two-way information sharing: The mechanism should allow for a mutually beneficial relationship, whereby the government receives information regarding security incidents and the private sector receives useful products such as early alerts and threat assessments.

5. Invest in an international training plan supported at high levels of government to address knowledge gaps. The plan could include short, medium, and long term exchange programs with relevant cyber security institutions, technical peer evaluations, and increased cooperation with international experts. The training plan should address the needs of officials from all government entities concerned with cybercrime and cyber security, as well as prosecutors, judges, and all other officials active in the area of law enforcement. This effort should be accompanied by regular briefings for high level officials to keep them abreast of developments in the field of cyber security and cybercrime.

6. Initiate a project and make use of existing relationships to facilitate the exchange of data regarding cyber security incidents. Colombia should implement this through relevant regional or international entities, e.g. the International Watch and Warning Network, the Forum for Incident Response and Security Teams.

7. In order to facilitate the rapid exchange of data related to cyber security and cybercrime, Colombia should adhere to the INTERPOL I-24/7 system for all cybercrime law enforcement units in Colombia.

8. Strengthen existing academic knowledge through international cooperation by jointly developing courses, visiting professorships, and student exchange programs that address cyber security risk management, incident management, network defense, forensic analysis, new technologies, etc.

9. Establish a framework to facilitate the direct exchange of data with Computer Emergency Response Teams outside of Colombia.

10. Identify counterparts in the region where cooperation and the establishment of confidence building measures would be mutually beneficial.

11. Actively participate in international cyber security fora to advance the goals identified in the international cooperation strategy. Actively encourage the establishment of and participation in technical exercises on a regional and global level on a regular basis.

12. Ensure that all international activities involving the exchange of personal data respect international human rights law, including the right to privacy.

Organization of American States (OAS)
Cyber Security Program