Organization of American States (OAS)

Last Updated: November 2020

Member States

POLICY

Strategy Documents

Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity

Inter-American Committee against Terrorism (CICTE), Inter-American Telecommunication Commission (CITEL), Meeting of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA).

- Adopted by the OAS General Assembly resolution AG/RES.2004 (XXXIV-O/04)
- Envisages three lines of action:
  - Creation of a Hemispheric Network of Computer Security Incident Response Teams (CSIRTs)
  - Identification and adoption of technical standards for a secure Internet architecture
  - 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

Source Source 2

8 June 2004

Other Documents

Research and Reports on Cybersecurity

Cybersecurity Programme; Inter-American Committee against Terrorism (CICTE)

- A series of research publications and reports on cybersecurity-related topics has been prepared by the OAS Cybersecurity Programme to its task of strengthening the capacities and level of awareness in relation to the growing threats to digital security pursuant to the objective of strengthening the capacities and level of awareness in relation to the growing threats to digital security in Americas and the Caribbean
- The list of publications and reports by topics includes :
  - **Cybersecurity in the banking sector:** State of cybersecurity in the banking sector in Latin America and the Caribbean (2018)
  - **Infrastructure protection:** Critical Infrastructure Protection in Latin America and the Caribbean (OAS-Microsoft, 2018)
  - **Cybersecurity incidents:** Study on the impact of digital incidents in Colombia (2017)
  - **Cybersecurity in Latin America and the Caribbean:** Cybersecurity: Are we ready in Latin America and the Caribbean? (2016)
  - **Critical infrastructure:** Cybersecurity and Critical Infrastructure in the Americas (OAS-Trend Micro 2015)
  - **Cybersecurity trends:** Latin American and Caribbean Cyber Security Trends (OAS-Symantec 2014)

Source

Starting from 2014

OAS White paper series

General Secretariat; Secretariat for Multidimensional Security (SMS)

- In October 2017, a joint agreement to advance cybersecurity education efforts was signed between OAS and Amazon Web Services (AWS)
- Pursuant to the agreement goals, a series of White papers on cybersecurity and cyber risk related topics were publised in partnership between OAS and AWS in 2018
- The White paper series aims at increasing the level of awareness among the public and business leaders throughout the region of Americas and the Caribbean
- The list of published White papers include:
  - A call to city leaders: Making our cities smarter, safer, and more efficient
  - A call to action to protect citizens, the private sector and the Government
  - Managing National Cyber Risk
  - Opportunities and challenges for SMEs in Cybersecurity

Source Source 2

2018

Organization of American States (OAS)

Last Updated: November 2020

Best Practices for Establishing a National CSIRT

General Secretariat

- Discusses the process of managing a project for the creation and deployment of a National CSIRT, including approaches and considerations necessary to define its constitution, mission, vision, scope, services, timeframe, legal, and institutional or organizational aspects
- Outlines detailed descriptions of infrastructure, covering hardware, software, and technical procedures
- Analyzes different policies and procedures necessary for fluid CSIRT operation, including review and highlight of elements of existing CSIRT frameworks such as those developed by ENISA and GÉANT
- Discusses guidelines for membership and participation in certain international bodies, such as the Forum of Incident Response and Security Teams (FIRST)

Source

April 2016

Communications

Declaration on Strengthening Hemispheric Cooperation and Development in Cybersecurity and Fighting Terrorism in The Americas

Inter-American Committee against Terrorism (CICTE)

- Adopted at the Sixteenth Regular Session of CICTE at the OAS Headquarters, Washington, D.C.
- In the declaration, the OAS member countries:
  - Declare their commitment to creating confidence-building measures that strengthen international peace and security and that can increase cooperation, transparency, predictability, and stability among states in the use of cyberspace, recognizing confidence and security building measures as one of the lynchpins of collaboration among member states which enhance trust and cooperation and reduce the risk of conflict
  - Recognize that the threat of terrorism is exacerbated when connections exist between terrorism and illicit drug trafficking, cybercrime, illicit arms trafficking, money laundering, and other forms of transnational organized crime, and that such illicit activities may be used to support and finance terrorist activities
  - Reiterate their commitment to prevent, combat, and eliminate terrorism through the broadest possible cooperation, with full respect for the sovereignty of states and in compliance with their obligations under national and international law, including international human rights law, international humanitarian law, and international refugee law

Source Source 2

26 February 2016

Declaration on the Protection of Critical Infrastructure from Emerging Threats

Inter-American Committee against Terrorism (CICTE)

- Adopted by the OAS member states at the CICTE´s Fifteenth Regular Session
- In the declaration, the OAS member countries:
  - establish their commitment to identifying and combating emerging terrorist threats, regardless of their origin or motivation, such as threats to critical infrastructure, and cyber security, among others
  - declare their willingness to identify and promote, when deemed appropriate, in accordance with domestic laws, forms of public-private partnerships in the fight against terrorism, and in connection with critical infrastructure and cyber security
  - urge the OAS member states who have not yet done so, to sign, ratify, or accede to as the case may be, and to implement in an effective way, the Inter-American Convention against Terrorism, and the other pertinent universal legal instruments, as well as the resolutions of the UN GA and Security Council related to combating terrorism

Source Source 2

20 March 2015

Declaration on Strengthening Cyber-Security in the Americas

Inter-American Committee against Terrorism (CICTE)

- Condemns terrorism
- Reaffirms commitment to implement the OAS Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity
- Asserts the need for all member states to continue their efforts to establish, and/or strengthen national cyber incident alert, watch, and warning groups (CSIRTs)

Source

Organization of American States (OAS)

Last Updated: November 2020

7 March 2012

STRUCTURE

Specialized Agencies

Inter-American Committee against Terrorism (CICTE)
Secretary General

- Condemns terrorism
- Reaffirms commitment to implement the OAS Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity
- Provides political and technical assistance to its member states in different areas agreed to in its annual Work Plan, including Cybersecurit
- Main functions include:
  - Provide technical and administrative support for CICTE sessions and maintain communication and coordination between sessions
  - Provide technical assistance and training to member states in response to their needs and requests
  - Coordinate activities with other international, regional and subregional organizations
  - Assert the need for all member states to continue their efforts to establish, and/or strengthen national cyber incident alert, watch, and warning groups (CSIRTs)

Source Source 2

7 June 1999 (established)

Key Positions

Cyber Security Program Manager
Secretariat, the Inter-American Committee against Terrorism (CICTE)

- Provides programmatic and management support to the CICTE Secretariat in the planning, organization and execution of cyber security initiatives in the Americas including:
  - Creation and Development of Computer Emergency Response Teams (CERTs)
  - Provision of Technical Training; Implementation of Crisis Management Exercises
  - Capacity building on Industrial Control Systems (ICS); and
  - coordinating outreach and collaboration with other international and regional organizations working on cyber issues

Source

Secretary for Multidimensional Security
Secretariat for Multidimensional Security (SMS); Ms. Farah Diva Urrutia

- Leads the Executive Office of the Secretary for Multidimensional Security at the Secretariat for Multidimensional Security (SMS)
- Works to implement the Secretariat's Mission: to promote and coordinate cooperation among the OAS member states and between them and the inter-American system and other bodies in the international system, in order to assess, prevent, confront, and respond effectively to threats to security, with a view to being the leading point of reference in the Hemisphere for developing cooperation and capacity-building in the OAS member states
- Coordinates acitivities of the Secretariat defined by the Declaration on Security in the Americas and its new concept of hemispheric security as being multidimensional and comprising traditional threats and new threats, concerns, and challenges to the security of the states of the Hemisphere

Source Source 2

16 July 2018 (acting Secretary appointed)

Executive Secretary of the Inter-American Committee against Terrorism (CICTE)
Inter-American Committee against Terrorism (CICTE); Secretariat for Multidimensional Security (SMS); Ms. Alison August Treppel

- Appointed by the Secretary General of the OAS to lead the CICTE Secretariat
- Responsible for promoting the Organization’s counter terrorism agenda throughout Latin America and the Caribbean, including activities in

Organization of American States (OAS)

Last Updated: November 2020

Cybersecurity
- Manages the day-to-day operations of the CICTE Secretariat

Source Source 2

October 2002 (position established); August 2016 (acting Executive Secretary appointed)

LEGISLATION

COOPERATION

Meetings

Meetings of Government Experts on Cyber Crime (Working Group on Cyber-Crime)

- Strengthens international cooperation in the prevention, investigation and prosecution of cybercrime, facilitate the exchange of information and experiences among its members, and make necessary recommendations to enhance and ensure efforts to combat these crimes
- Last meeting (IX) took place in December 2016

Source

1999-2016

Meetings of Ministers of Justice or other Ministers or Attorney General of the Americas and Cyber Crime

General Assembly

- The Meetings of Ministers of Justice or other Ministers or Attorneys General of the Americas (Spanish acronym REMJA), was for the first time conceived during the 27th Regular Session of the General Assembly of the OAS in Lima, Peru (1997)
- The REMJA is:
  - attended by the Ministers of Justice, other Ministers, or Attorneys General, with responsibilities in the area of public policy regarding justice matters, as well as international legal cooperation, particularly with regard to criminal matters, from the 34 OAS Member States
  - supported by the OAS Department of Legal Cooperation of the Secretariat for Legal Affairs
  - structured around a high-level dialogue at the Ministerial level, which allows for direct and horizontal cooperation between OAS member States

Source Source 2

December 1997 (first meeting); 28 - 30 April 2008 (last meeting)

Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace

- The Working Group on Cooperation and CBMs in Cyberspace was established by CICTE through Resolution CICTE/RES.1/17 on April 7, 2017 with the mandate to prepare a set of draft confidence-building measures (CBMs), based on the consensus reports of the UN GGE, and report its advances and activities to CICTE and the Committee on Hemispheric Security of the OAS
- At the first meeting of the WG on February 28-March 1, 2018, a Draft Set of "Cyber CBMs for the Inter-American System" was presented to the WG for their consideration; these proposed Cyber CBMs were agreed to with a proposed plan of action to establish additional measures
- In accordance with the Resolution AG/RES. 2925 (XLVIII-O/18) adopted on June 5, 2018, the OAS General Assembly agreed to adopt the recommendation of the WG and the CICTE Plenary, in which Member States agreed, inter alia, to the following two priority voluntary cyber CBMs:
  - Provide information on cybersecurity policies, such as national strategies, white papers, legal frameworks, and other relevant documents
  - Nominate a national point of contact at the policy level able to discuss the implications of hemispheric cyber threats
- Member States also acknowledged the benefits of continuing the WG as an ongoing mechanism and agree to continue to meet to establish the requisite procedures for continuing discussion of new and agreed-upon cyber CBMs

Source Source 2

February 28-March 1, 2018 (Meeting)

Activities

Organization of American States (OAS)

Last Updated: November 2020

OAS Cyber Security Programme

Inter-American Committee against Terrorism (CICTE)

- Goals:
  - Support OAS member states in the development of technical and political capacities to prevent, identify, respond to and recover from cyber-incidents
  - Improve the exchange of information, cooperation and coordination among cybersecurity stakeholders at the national, regional and international levels
  - Increase access to knowledge and information about threats and cyber risks by public, private and civil society stakeholders, as well as internet users
- Addresses cyber security issues based on a flexible and dynamic approach, with focus on three core areas:
  - **Policy development:** Helps OAS member states to develop cybersecurity strategies that involve all relevant stakeholders and that adjust to the legislative, cultural, economic and structural situation of each country and support the national assessments of the capacity and maturity of cybersecurity. Under this path, the program supports the development of confidence-building measures in cyberspace.
  - **Capacity building:** Helps establish and develop the capacity of existing national computer security incident response (CSIRT) teams and provides personalized technical assistance and exercise opportunities to strengthen national and regional institutions and organizations. The development of a cybersecurity workforce is also carried out through various forms of professional development opportunities.
  - **Research and Outreach:** Develops technical documents, toolkits and research-based reports to guide policy makers, CSIRTs, infrastructure operators, private organizations and civil society, highlighting current developments and identifying key cybersecurity challenges in the region

Source Source 2

Inter-American Cooperation Portal on Cyber-Crime

Ministers or Attorneys General of the Americas (REMJA) Technical Secretariat

- Launched to facilitate and streamline cooperation and information exchange among government experts from OAS Member States with responsibilities in the area of cybercrime or in international cooperation for its investigation and prosecution
- Consists of:
  - *Public component*: data on national legislation of OAS Member States in the area of cybercrime, as well as on action taken within the OAS related to training workshops, WG meetings, and other technical cooperation activities
  - *Private component:* information exclusively of interest to the government experts from OAS Member States with responsibilities in the area of cybercrime or in international cooperation for its investigation and prosecution
- The Portal's public component includes:
  1. Cybercrime related useful document directory
  2. Questionnaires on cyber crime and replies from Member States
  3. Directory of national points of contact (POC) on cybercrime in the Member States
  4. Materials from Technical Workshops of the WG on Cybercrime
  5. Calendar of Meetings of Government Experts on Cyber Crime
  6. Information on the OAS country developments in cybercrime area

Source

Hemispheric Network of Computer Security Incident Response Teams (CSIRTs) (OAS Hemispheric Network)

OAS Cybersecurity Program

- Online platform designed to:
  - Facilitate real-time communication and information sharing
  - Provide early warning feeds and alerts
  - Identify incident trends in the region
  - Facilitate online and real-time collaboration between national CSIRTs
  - Provide virtual sandboxes to develop tools
- Membership includes national, police, defense and government CSIRTs from Americas

Source Source 2

2016 (launched)

External Cooperation

Organization of American States (OAS)

Last Updated: November 2020

Global Forum on Cyber Expertise (GFCE), Membership

- GFCE is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building
- OAS participates in the following GFCE initiatives:
  - Assessing and developing cybersecurity capability
  - Cyber Security Initiative in OAS member states
  - CSIRT Maturity Initiative

Source Source 2

2015 (established)

Internet Corporation for Assigned Names and Numbers (ICANN) Governmetnal Advisory Committee (GAC) - Membership

Inter-American Committee against Terrorism (CICTE)

- The Governmetnal Advisory Committee (GAC) is an advisory committee to the Internet Corporation for Assigned Names and Numbers (ICANN), created under the ICANN ByLaws
- The GAC provides advice to ICANN on public policy aspects of ICANN's responsibilities with regard to the Internet Domain Name System (DNS)
- The GAC is not a decision-making body; it advises ICANN on issues that are within ICANN's scope.
- The OAS sits as an observer organization with GAC

Source