Organization of American States

INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)

SIXTEENTH REGULAR SESSION
February 25-26, 2016
Washington, D.C.

OEA/Ser.L/X.2.16
CICTE/Dec 1/16
26 February 2016
Original: Spanish

DECLARATION

STRENGTHENING HEMISPHERIC COOPERATION AND DEVELOPMENT IN CYBERSECURITY AND FIGHTING TERRORISM IN THE AMERICAS

(Approved at the Fifth Plenary Session held on February 26, 2016)

DECLARATION

STRENGTHENING HEMISPHERIC COOPERATION AND DEVELOPMENT IN CYBERSECURITY AND FIGHTING TERRORISM IN THE AMERICAS

(Approved at the Fifth Plenary Session held on February 26, 2016)

THE MEMBER STATES OF THE INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE) of the Organization of American States (OAS), meeting at its sixteenth regular session, held in Washington, D.C., in the United States of America, on February 25 and 26, 2016:

1. REAFFIRMING the nature, principles, and purposes of the Inter-American Committee against Terrorism (CICTE) and reiterating their strongest condemnation of terrorism in all its forms and manifestations, regardless of its origins and manifestations, in accordance with the principles of the Charter of the Organization of American States and of the Inter-American Convention against Terrorism, and with full respect for the sovereignty of states, the rule of law, and international law, including international humanitarian law, international human rights law, and international refugee law;

2. RECOGNIZING 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;

3. REAFFIRMING all the declarations adopted at the sessions of the Inter-American Committee against Terrorism and reconizing all the resolutions on terrorism adopted by the OAS General Assembly;

4. ALSO REAFFIRMING resolution AG/RES. 1939 (XXXIII-0/03), "Development of an Inter-American Strategy to Combat Threats to Cybersecurity," and reaffirming resolution AG/RES. 2004 (XXXIV-0/04), "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity";

5. ENDORSING the international counter-terrorism framework adopted by the United Nations through the resolutions of the General Assembly and of the Security Council and in the Global Counter-Terrorism Strategy;

6. EMPHASIZING the importance of the OAS Member States signing, ratifying, or acceding to, as the case may be, and implementing in an effective way the Inter-American Convention against Terrorism as well as the pertinent universal instruments, including the United Nations Conventions, pertinent Resolutions of the Security Council and Human Rights Council of the United Nations, and the United Nations Global Counter-Terrorism Strategy adopted by the General Assembly of said organization;

7. DEVELOPING a culture of cybersecurity in the Americas by taking effective preventive measures to anticipate, address, and respond to cyberattacks, whatever their origin, and regardless of who commits them, fighting against cyber threats and cybercrime, criminilazing attacks against cyberspace, protecting critical infrastructure and securing networked systems. Reafirming our commitment to develop and implement and integral OAS cybersecurity strategy, utilizing the contributions and recommendations developed jointly by member state experts and the REMJA Governmental Expert Group on Cybercrime, CICTE, the Inter-American Telecommunication Commission (CITEL), and other appropriate organs, taking into consideration the existing work developed by member states, coordinated with the Committee on Hemispheric Security;

8 RECALLING that the Ministers of Public Security of the Americas meeting in MISPA V, held on November 19-20, 2015 in Lima, issued a statement reaffirming their decided and firm commitment with peace and the fight against terrorism in all its forms and manifestations;

9. RECOGNIZING that the fight against terrorism requires criminal justice systems that respect and protecthuman rights and fundamental freedoms, in order to ensure that individuals who plan, carry out, or support acts of terrorism are brought to justice, wherever they may be, and be subject to due process;

10. UNDERSCORING their support for and solidarity toward the victims of terrorism and their families, together with the importance of providing them with appropriate assistance and protection in accordance with domestic law of each state;

11. MINDFUL of the declaration "Strengthening Cybersecurity in the Americas," adopted at the fourth plenary session of the twelfth regular session of CICTE on March 7, 2012, and of the declaration "Protecting Critical Infrastructure from Emerging Threats," adopted at the fifth plenary session of the fifteenth regular session of CICTE on March 20, 2015;

12. NOTING WITH SATISFACTION the extensive work carried out by the CICTE Secretariat as well as the working group on cybercrime of the REMJA, and CITEL since 2004 to implement the aforesaid Inter-American Strategy to Combat Threats to Cybersecurity**,** as well as the implementation of the CICTE Work Plan, which includes the topic of Protecting Critical Infrastructure and, within it, the Cybersecurity Program;

13. REITERATING the importance of continuing to implement the aforesaid Strategy and the need to strengthen partnerships between all cybersecurity stakeholders;

14. RECOGNIZING that free expression and the free flow of information, exercised in accordance with member states' applicable obligations and commitments within the framework of international and regional human rights instruments, are essential for innovation and for the operation of the computer networks that underpin economic growth and social development;

15. RECOGNIZING ALSO that the member states are making increased use of the infrastructure of information and communications technologies (ICTs), networks, information systems, and related technologies, integrated into the global network of the internet, and that this increases

the possible impact on the member states of threats to cybersecurity and the exploitation of related vulnerabilities;

16. CONSIDERING, therefore, that the appropriate development of capacities and frameworks for cybersecurity and ICT infrastructure is essential for regional, national, and individual security and for socioeconomic development;

17. AWARE that states must not pursue or deliberately support activities in the realm of information and communications technologies (ICTs) contrary to their obligations under international law that could intentionally damage criticalinfrastructure;

18. RECOGNIZING the work carried out by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and taking note of the reports prepared by that group (2010, 2013, 2015);

19. TAKING Note of Resolution A/70/125 of the United Nations General Assembly and the final document of the High-Level Meeting on the General Review of the Application of the Results of the Global Summit on the Information Society, particularly the priority given to building confidence and security in the use of information and communication technologies;

20. MINDFUL of the need to continue strengthening the CICTE Secretariat in its role of supporting the Member States and enhancing their capacity to cooperate to prevent, combat, and eliminate terrorism;

21. UNDERSCORING the importance of activities, projects, and programs developed in its various work areasby CICTE established in their yearly work plans, in particular, the realization of workshops, seminars, meetings, traninnings, special courses and other related activities at the national, sub regional and regional level;

22. CONSIDERING the importance of member states cooperating with key stakeholders in the use of cyberspace, such as the private sector, civil society, academia, the technical community, among other stakeholders and international organizations;

DECLARE:

1. Their most vehement condemnation of terrorism, and those who support it, in all its forms and manifestations, for being a criminal and unjustifiable act, under any circumstances, regardless of where and by whom it is committed, and because it constitutes a serious threat to international peace and security and to the democracy, stability, and prosperity of the region’s countries;

2. Their determined 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;

3. That they urge those member states that have not yet done so to sign, ratify, or accede to, as the case may be, the Inter-American Convention against Terrorism and the other pertinent universal legal instruments, and to implement in an effective manner the antiterrorism resolutions of the United Nations General Assembly and Security Council;

4. Their renewed commitment to implement the Inter-American Cybersecurity Strategy, adopted by means of resolution AG/RES. 2004 (XXXIV-O/04) US: in which member states reaffirmed their commitment to develop and implement an integral OAS cyber security strategy, utilizing the contributions and recommendations developed jointly by member state experts and REMJA Governmental Experts Group on Cybercrime, CICTE, the Inter-American Telecommunication Commission (CICTEL), and other appropriate organs, taking into consideration the existing work developed by member states, coordinated with the Committee on Hemispheric Security;

5. The importance of acknowledging the Internetas a global facility along with developing measures for promoting an open, secure, and peaceful ICT environmentunderstanding the Internet and its security as crucial elements for the development of the member states' economies and as a key factor for improving the integration of information systems in our region;

6. The importance of ensuring and reaffirming the full respect of Human Rights in the use of cyberspace, as enshrined in different instruments such as the Universal Declaration of Human Rights, and particularly those set out in the American Convention on Human Rights for parties thereto, bearing in mind its interdependency, equality and indisivilityand, to that end, increasing forums for cooperation with the Inter-American Commission on Human Rights and its rapporteurships to assist with those tasks;

7. The need for all the member states to continue with their efforts to establish and/or strengthen national alert, monitoring, and response groups for cybersecurity incidents, known as Computer Security Incident Response Teams (CSIRTs);

8. The importance of the member states participating in and strengthening the hemispheric security network of the CSIRTs and cybersecurity authorities, and of the member states increasing their exchanges of information and their cooperation related to the protection of critical information infrastructure and for the prevention of and response to cybersecurity incidents;

9. Their commitment to urging the competent law enforcement institutions to participate in the Networkand to keep it updated;

10. The importance of creating frameworks and protocolsfor cooperation and assistance among the member states, for when incidents occur in one member state and their effects are felt in others;

11. 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 securitybuilding measures as one of the lynchpins of collaboration among member states which enhance trust and cooperation and reduce the risk of conflict;

12. The importance of bolstering the security and the capacity for recoveryof critical information and communications technology (ICT) infrastructure in connection with cyberspace risks, with particular emphasis on critical government institutions and other public and private sectors that are critical for national security, includingdigital government, health, energy, financial, telecommunications, and transportation systems and others, through the use of cyber and physical measures;

13. The importance for all the member to create and/or strengthen specialized units within their relevant law enforcement agencies for the prevention and investigationof cibersecurity incidents;

14. Their willingness to provide assistance and training for improving security in the use of information and communications technologies (ICTs), and to share their best technical, legal, and administrative practices to that end;

15. The need to establish procedures for mutual assistance when responding to incidents, in addressing short-term network security problems, and provide collaboration with the reciprocal requests made by the member countries in order to investigate and prosecute crime related to terrorist acts, including procedures for expediting that assistance;

16. The importance of facilitating crossborder cooperation to address basic infrastructure vulnerabilities that transcend national borders;

17. To request that the CICTE Secretariat, within its competencies continue its work of strengtheningmember state' capacity to prevent**,** respond and deal with the use of information and communications technologies (ICTs) for terrorist while respecting human rights together with its work to raise internet users' awareness regarding risks in cyberspace;

18. Their willingness to create and/or strengthen awareness programs and campaigns, targeting in particular those groups that are most vulnerable to cybercrime;

19. The need for the CICTE Secretariat to continue, within its competencies, developing the member states'capacity, that so request it, to fight terrorist incidents or actsincluding initiatives for prevention, responding to cyber incidents, carrying out investigations and evidence analysis, international cooperation in response and investigation, and other activities that will serve to strengthen the capacity of the agencies responsible for law enforcement and responding to cyber incidents in the Americas;

20. The need for the CICTE Secretariat, within its competencies**, ,** in accordance with the 2004 Comprehensive Inter-American Cybersecurity Strategy (the 2004 Strategy and its Appendix A) to continue developing cooperation mechanisms with other international agencies and organizations in order to take coordinated actions for the protection and use of cyberspace;

21. Their willingness to continue developing comprehensive national cybersecurity strategies and to involve all relevant actors and stakeholders in their development and implantation, including, the private sector, academia, the technical community and civil society among others;

22. The importance of promoting cooperation among the public and private sectors, academia, the technical community, civil society, and other social actors to strengthen the safekeeping and protection of that critical information and communications infrastructure;

23. To explore future opportunities for expanding CICTE's efforts at building the capacity of member statesto protect information and communications infrastructure systems, including the implementation of capacity-building programs to strengthen the security of global supply chains;

24. To urge member states to make voluntary contributions to strengthen CICTE's ability to assist the member states, when they so request, in implementing the 2004 Strategy and its Appendix A**,** approved declarations and the Work Planand this Declaration;

25. To invite the member states, permanent observers, and pertinent international organizations provide, maintain, or increase, as appropriate, their voluntary financial or human resource contributions to CICTE, to facilitate the performance of its duties and promote the enhancement of its programs and the scope of its work;

26. Their interest in creating a voluntary contribution fund, through which the member states, permanent observers, and pertinent international organizations would be able to make voluntary financial contributions to increase cybersecurity in the Americas, and to instruct the CICTE Secretariat to submit a draft of its operating rules to the Committee on Hemispheric Security;

27. Their request that the OAS General Assembly instruct the General Secretariat, within the resources allocated in the program-budget of the OAS, to provide the CICTE Secretariat with the human and financial resources necessary to implement the CICTE Work Plan, including the areas dealing with Border Controls, Legislative Assistance and Combating Terrorism Financing, Protection of Critical Infrastructure, Strengthening Strategies on Emerging Terrorist Threats, and International Coordination and Cooperation;

28. To instruct the CICTE Secretariat, within its competencies, support the member statesthat so request itwith their commitment and efforts in complying with and implementing this declaration and the CICTE Work Plan;