Organization of American States

INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)

FIFTEENTH REGULAR SESSION
March 19-20, 2015
Washington, D.C.

OEA/Ser.L/X.2.15
CICTE/doc.1/15
23 March 2015
Original: Spanish

DECLARATION

PROTECTION OF CRITICAL INFRASTRUCTURE FROM EMERGING THREATS

(Approved at the Fifth Plenary Session held on March 20, 2015)

DECLARATION

PROTECTION OF CRITICAL INFRASTRUCTURE FROM EMERGING THREATS

(Approved at the Fifth Plenary Session held on March 20, 2015)

THE MEMBER STATES OF THE INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE) OF THE ORGANIZATION OF AMERICAN STATES (OAS), gathered at its fifteenth regular session, held in Washington, D.C., in the United States of America, from March 19 to 20, 2015:

1. RECOGNIZING the content of United Nations Security Council Resolution 2178 which reaffirms that terrorism in all forms and manifestations constitutes one of the most serious threats to international peace and security, and that any acts of terrorism are criminal and unjustifiable regardless of their motivations, whenever and by whomsoever committed; and remaining determined to contribute further to enhancing the effectiveness of the overall effort to fight this scourge on a global level;

2. REAFFIRMING their commitment to preventing, combating, and eliminating terrorism and its funding, according to the principles of the Charter of the Organization of American States and of the Inter-American Convention against Terrorism, with full respect for national sovereignty, the rule of law, and international law, including international humanitarian law, international human rights law, and international refugee law;

3. RENEWING THE COMMITMENTS assumed in the Declaration of Panama on the Protection of Critical Infrastructure in the Hemisphere in the Face of Terrorism (CICTE/DEC.1/07) and in all the declarations adopted at the meetings of the Inter-American Committee against Terrorism, and recognizing all the resolutions adopted by the OAS General Assembly and Permanent Council in connection with terrorism;

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

5. RECOGNIZING the content of the 2013 CICTE Declaration that the importance for member states of the OAS to sign, ratify, or accede to, as the case may be, and to implement in an effective way the Inter-American Convention against Terrorism, as well as the pertinent universal legal instruments, including all the existing related international conventions, protocols, and amendment, and to implement the UN Security Council resolutions 1267 (1999), 1373 (2001), 1540 (2004), 1624 (2005), 1631 (2005), 2133 (2014), 2178 (2014), 2170 (2014) and other pertinent resolutions, and the UN Global Counter-Terrorism Strategy adopted by the UN General Assembly;

6. NOTING WITH CONCERN that the terrorism threat has become more diffuse, with an increase of terrorist acts in various regions of the world, including those motivated by intolerance or extremism; and EXPRESSING their determination to combat this threat;

7. TAKING INTO ACCOUNT that the threat of terrorism would be exacerbated in those cases in which connections may be established between terrorism and illicit drug trafficking, illicit trafficking in arms, money laundering, and other forms of transnational organized crime, and that such illicit activities might be used to support and finance terrorist activities;

8. EMPHASIZING that terrorism cannot and should not be associated with any religion, nationality, or civilization;

9. RECOGNIZING the content of United Nations Security Council Resolution 2178 which reaffirms concern over the increased use by terrorists and their supporters of communications technology for the purpose of radicalizing to terrorism, recruiting and inciting others to commit terrorist acts, including through the internet, and financing and facilitating the travel and subsequent activities of foreign terrorist fighters and underlining the need for Member States to act cooperatively to prevent terrorists from exploiting technology communications and resources to incite support for terrorist acts,

while respecting human rights and fundamental freedoms and in compliance with other obligations under international law;

10. HIGHLIGHTING the need for member states to act cooperatively to prevent terrorists from exploiting technology, communications, and resources to incite support for terrorist acts, developing this cooperation in strict observance of human rights, privacy rights and fundamental freedoms, while respecting national sovereignty;

11. BEARING IN MIND That critical infrastructure refers, inter alia, to those facilities, systems, and networks, and physical or virtual (IT) services and equipment, the disabling or destruction of which would have a severe impact on populations, public health, security, economic activity, the environment, government services or the ability of the government of a Member State to operate effectively and that any interruption thereof caused by terrorist acts would have grave consequences for the flow of essential services and the functioning of supply chains;

12. UNDERSCORING that new technologies and regulatory gaps in new payment methods have proven not to be immune from risk of being abused for the purposes of terrorist activities;

13. UNDERSCORING that protecting critical infrastructure against terrorist attacks and other emerging threats such as the use of the Internet for terrorist purposes among others and ensuring that they operate normally is a concern to the member states that demands the implementation of security programs that include the resilience of critical infrastructure based on risk analysis developed in cooperation with stakeholders, through exchanges of good practices and experiences, in order to ensure the security of that infrastructure; and that such undertakings are a shared responsibility of public and private actors requiring awareness and cooperation and collaboration among them;

14. RECALLING the recommendations of the Meeting of Experts on Tourism and recreational services security that took place in March, 2008 in anticipation of CICTE VIII; the Declaration of Port of Spain, adopted at the Fifth Regular Session of CICTE; the mandates established by OAS General Secretariat Resolution 2137 of June 2005;

Resolution 2397 adopted in 2008 on the Special Security Concerns of the Small Island States of the Caribbean, other OAS General Assembly Resolutions that approved the CICTE Work Plan, which included Tourism Security; considering that the Tourism Sector is a critical infrastructure and its immense contributions to global competitiveness, national income, employment generation and sustainable development in many Member States throughout the Hemisphere;

15. AWARE of the need to continue strengthening the CICTE Secretariat in its role of supporting member states and to enhance their capacity to cooperate to prevent and counter all forms and manifestations of terrorism;

16. REAFFIRMING that the fight against terrorism demands the broadest possible cooperation among the member states and coordination among international and regional organizations, in order to prevent, punish, and eliminate terrorism in all its forms;

17. AWARE OF a comprehensive Inter-American Cybersecurity Strategy: a multidimensional and multidisciplinary approach to creating a culture of Cybersecurity,

DECLARE:

1. Their most vehement condemnation of terrorism in all its forms and manifestations, as they consider it criminal and unjustifiable, regardless of their motivations and where and by whom it is committed, and because it constitutes one of the most serious threat**s** to life and to international peace and security, and to the democracy, stability, and prosperity of states; and their remaining determined to contribute further to enhancing the effectiveness of the overall effort to fight this scourge on a global level.

2. 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.

3. Their commitment to identifying and combating emerging terrorist threats, regardless of their origin or motivation, such as threats to critical infrastructure, and cybersecurity, among others and the need for private sector cooperation to prevent, develop resilience of critical infrastructure, and facilitate the resolution of terrorist and related crimes that are committed through global communication networks.

4. Their willingness to identify and promote, when deemed appropriate, in accordance with domestic laws, forms of public-private partnership~~s~~ in the fight against terrorism, in connection with critical infrastructure and cybersecurity.

5. Their firm commitment to strengthen national and multilateral efforts, to prevent, combat, and eliminate terrorist threats and attacks against critical financial, transportation, and telecommunications infrastructure.

6. Their further commitment to continue providing support for the provision of technical assistance and capacity-building to Member States related specifically to the security practices of the tourism and recreational sectors, which incorporate competitive standards, preventive security and perception, contingency planning and management, victim assistance, the role of the media and communication during a crisis, and public health and emergency response.

7. Their commitment to strengthening international cooperation and collaboration mechanisms, in light of the national, regional, and global interdependence of critical infrastructure and in recognition of the importance of implementing effective and coordinated actions for the continued improvement of the protection and the resilience of these critical infrastructures.

8. Their commitment to identifying and fighting real and emerging terrorist threats regardless of their origin, such as the use of the Internet for terrorist, bioterrorism, and threats to tourism security and critical infrastructure, as defined by each State, and the possibility of the access to and possession, transportation, and use of weapons of mass

destruction and related materials and their vectors in the hands of terrorists, and to promote the formulation and adoption of cooperation programs.

9. To instruct the Executive Secretariat of the Inter-American Committee against Terrorism (CICTE), at the request of those member states that so wish, to develop a technical assistance project that, will allow those states to prepare a categorized list of their critical infrastructure, based on the corresponding assets, systems, networks, and essential functions, in order to better assess vulnerabilities, shortcomings, threats, risks, and interdependence for the development of plans for its optimal protection through exchanges of good practices and experiences.

10. To also instruct the Executive Secretariat of CICTE at the request of those member states that so wish, to develop a technical assistance project that, will allow these states to prepare a categorized list to identify, products and/or electronic payment services with an evident lack of control and oversight from the competent authorities, with a view to highlight the risks that they pose with respect to terrorist activities.

11. Their commitment to effectively implement the International Ship and Port Security Code (ISPS), which is binding upon the contracting states of the International Maritime Organization (IMO), as well with the 1944 Chicago Convention, "Safeguarding International Civil Aviation against Acts of Unlawful Interference," of the Civil Aviation Organization (ICAO).

12. Instruct the CICTE Secretariat to consider support for those member states that so request in their efforts to prevent and combat the use of communications technologies, particularly the internet, for the purposes of radicalizing recruiting, and inciting others to commit terrorist acts, while respecting at the same time human rights and fundamental freedoms and complying with other obligations under international law.

13. Request that the Committee on Hemispheric Security consider holding a session in order to encourage awareness on the importance of critical infrastructure security.

14. Underline the importance of the role played by National Points of Contacts, among them Ministries of Foreign Relations and other Member State departments and organizations, in the prevention and eradication of terrorism and in making possible further cooperation among Governments, and with CICTE to improve the conditions to carry out an ever more efficient fight against this scourge.

15. To urge the OAS Regular Fund to contribute the necessary resources to provide the CICTE Secretariat with human and financial resources to ensure continuity in its endeavors and the implementation of its mandates, programs, and activities contained in the Work Plan adopted at the fifteenth regular session.

16. To request member states, permanent observers, and pertinent international organizations to provide, maintain, or increase, as appropriate, their voluntary financial and/or human resource contributions to CICTE, in order to facilitate the performance of its functions and promote the enhancement of its programs and the scope of its work.

17. Their commitment to implementing this Declaration and the CICTE Work Plan, which includes areas of work in identifying pieces of critical infrastructure with vulnerabilities, threats, or risks that can be minimized or eliminated by means of exchanges of good practices and experiences.