CTED contribution to the report of the Secretary-General on oceans and the law of the sea

I. Introduction

1. The border security-related obligations set forth in Security Council resolution 1373 (2001) require action in a number of areas, including in the area of maritime security. Effective border management is of particular importance in preventing and disrupting the movement of foreign terrorist fighters (FTFs), as emphasized by the Security Council in its resolutions 2178 (2014) and 2396 (2017). Border security includes controls on the movement of people and goods across borders, as well as the prevention of unlawful interference in maritime navigation and international cargo movement.

2. It is vitally important that States put in place sufficient maritime border-management capacities and, more broadly, specific legal frameworks and operational measures to detect and prevent the cross-border movement of individuals who pose a terrorism-related threat, as well as the cross-border movement of licit and illicit cargo that might be used for terrorist purposes. Effective and efficient screening of travellers at ports of entry requires a combination of several mechanisms, depending on whether the border in question is aerial, maritime or land border. The key mechanisms in this context include advance passenger information (API), Passenger Name Records (PNR), biometric technology, risk assessment and targeting rules, and access to databases of the International Criminal Police Organization (INTERPOL). Special measures to enhance maritime security are also set forth in the International Ship and Port Facility Security (ISPS) Code, which is a mandatory instrument for the 148 contracting parties to the 1974 Safety of Life at Sea (SOLAS) Convention. The aim of the ISPS Code is to ensure that the applicable ocean-going vessels and port facilities of IMO member States are implementing the highest possible standards of security, according to a system of survey, verification, and control.

3. In its resolution 2341 (2017), the Security Council notes the increasing interdependency of States' cross-border critical infrastructures, such as those used for the generation, transmission and distribution of energy; air, land and maritime transport; banking and financial services; water supply; food distribution; and public health.

4. The guiding principles relating to border security and information-sharing set forth in the *Security Council Guiding Principles on Foreign Terrorist Fighters: the 2015 Madrid Guiding Principles + 2018 Addendum* (S/2015/939 and S/2018/117) are relevant to maritime security, including with respect to the need to make regular use of INTERPOL databases in screening travellers at maritime ports of entry and in order to strengthen investigations and risk assessments of returning and relocating FTFs and their families.

5. The Counter-Terrorism Committee Executive Directorate (CTED) addresses issues related to Maritime security in the counterterrorism context during its country assessments conducted on behalf of the Counter-Terrorism Committee. Maintaining secure maritime borders and policing sea and coastal areas can be extremely challenging for many Member States. The difficulty of effectively patrolling vast and porous marine borders and spaces is often compounded by the lack of physical borders and checkpoints. Other challenges derive from the lack of financial and human resources, equipment and specialist skills and /or the lack of intra-State and inter-State cooperation. Ensuring effective border security is an integral part

of any comprehensive and integrated national counter-terrorism strategy and requires collective action by States and relevant international and regional organizations. The Committee and CTED can assist States to identify and share good practices in this area and facilitate the delivery of technical assistance and financial support to ensure implementation of the relevant Council resolutions and the Committee's related recommendations on maritime security.

II. Main developments in the maritime domain since the last reporting period

6. CTED shares the Committee's recommendations on maritime security-related issues through the Global Counter-Terrorism Coordination Compact, established in 2018, and its online platform, launched in 2020, with member entities of the Compact. CTED also works closely together with the United Nations Office of Counter-Terrorism (UNOCT) and the International Maritime Organization (IMO) and other relevant partners within the framework of the Compact, in particular through its Working Group on Border Management and Law Enforcement Relating to Counter-Terrorism, which addresses issues relating to maritime security.

7. The maritime environment possesses certain unique characteristic that make it particularly alluring and vulnerable to terrorist and criminal organizations, especially as port facilities, ships and shipping lanes, and off-shore fixed platforms often constitute "critical infrastructure" (i.e., key nodes for the delivery of goods and services that are considered vital for the essential functioning of States' economies). Passenger ships also represent attractive and vulnerable targets. Owing to their capacity to accommodate high numbers of passengers and the lack of secure embarkation procedures, modern cruise ships and passenger ferries may also represent ideal "soft" targets for terrorist groups seeking to cause maximum damage and media coverage with limited planning and effort.

8. The maritime domain could benefit from increased attention by the international community and the adoption of robust security practices for States (e.g., in terms of passenger data collection and exchanges to detect the cross-border movement of terrorists) to close potential vulnerabilities and avoid exploitation as experienced in other modes of transportation.

9. The Private industry should be considered an integral partner to countering the maritime terrorist travel threat. The private sector can provide States with valuable information and risk and threat assessments. Similarly, States can provide the private sector with threat warnings, regulatory notices, and issue-specific data, subject to authorization.

10. CTED has established through its assessments and dialogue with Member States that there is a need to increase robust maritime domain awareness with respect to any risk associated with the global maritime environment that could adversely affect the security, safety, economy, or environment of a State. There is a need to explore challenges in collecting complete, accurate, and reliable data to support risk assessments, which should also include assessing risks stemming from foreign ports. Extending access to advance passenger information (API) and Passenger Name Records (PNR) to vet maritime travellers would further strengthen maritime-border protection. Although implementation of the requirements of the relevant Security Council resolutions on API and PNR for air borders had increased security in the air domain, the risk might move to the maritime and/or land border, as terrorists are continuously

looking to exploit the next vulnerability. Introduction of international API and PNR standards in the maritime domain would not be without challenges since the maritime domain presented its own specificities, including the variety of maritime carriers, types of traveller, booking systems, and check-in procedures involved. There are ongoing international efforts seeking to set standards for the transmission of personal data from Cruise Ships, both API and PNR.

11. In October 2022 during its Special Meeting, the Counter-Terrorism Committee (CTC) unanimously adopted the Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes. Among the listed items in the Declaration include the decision to continue to work on recommendations on the three themes of the Special meeting and the intention to develop a set of non-binding guiding principles to assist Member States to counter the threat posed by the use of new and emerging technologies for terrorist purposes. It is critical that Member States integrate new, emerging and evolving threats into their threat and risk assessments including in the maritime domain. In its resolution 2617(2021), the Security Council noted with concern the increasing global misuse of unmanned aerial systems (UAS) by terrorists to conduct attacks against, and incursions into, restricted commercial and government infrastructure and public places. Many Member States have expressed that their concerns over the potential threats posed by UAS to attack critical infrastructure, such as ports, but also underwater as a risk to maritime operations. At the same, UAS can be used for border security purposes including monitoring porous coastal borders, and conducting search and rescue operations.

12. CTED has contributed to the initiatives on Counter Maritime Terrorism and Enhance Maritime Security developed under the Global Counterterrorism Forum (GCTF).