United Nations Security Council
Counter-Terrorism Committee
Executive Directorate (CTED)

LAW ENFORCEMENT

Member States' law enforcement agencies must constantly adapt to a global terrorist threat that has evolved significantly over the past decades, both in scale and complexity. The current terrorism environment is marked in particular by increasingly sophisticated abuse of new and emerging technologies (including information and communications technologies (ICT)), continuing terrorist threats against critical infrastructure and "soft" targets, as well as the use of improvised explosive devices (IEDs) and unmanned aircraft systems (UAS) for terrorist purposes.

ADDITIONAL RESOURCES

The Compendium of good practices for the protection of critical infrastructures against terrorist attacks helps raise awareness of the requirements of resolution 2341 (2017). The Compendium provides Member states and international and regional organizations with guidelines and good practices on the protection of critical infrastructures against terrorist attacks (with indicators, standards, risk assessment measures, recommendations, good practices, and so forth). It also provides Member States with reference material on the development of strategies for reducing risks to critical infrastructure from terrorist attacks.

Security Council resolution 1373 (2001) requires Member States to "ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice". Furthermore, in its resolution 2322 (2016) the Council calls upon all States, among other things, to "exchange information, in accordance with international and domestic law and cooperate on administrative, police and judicial matters to prevent the commission of terrorist acts and to counter the foreign terrorist fighter (FTF) threat, including returnees". In order to comply with this requirement, it is essential that States establish fully functioning, efficient and professional law enforcement capacities, including dedicated or specialized counter-terrorism units, where appropriate. Because of the transnational nature of terrorism, these capacities must also be reflected at the regional and international levels.

In many ways, transnational law enforcement cooperation remains at the developmental stage. States often lack clear cooperation and information-sharing frameworks and protocols, as well as access and/or connectivity to information-sharing mechanisms such as regional and international counter-terrorism and criminal databases and networks. Such cooperation is crucial, however, especially when several States of the same region are exposed to the same or similar terrorist threat. One of CTED's focus areas is therefore to facilitate international and regional cooperation, ideally through the establishment of a regional mechanism that can bring together the law enforcement agencies of several States. Sharing of counter-terrorism information and access to data are also critical building blocks of national risk and threat assessments. The Security Council has recognized the proven effectiveness of the International Criminal Police Organization (INTERPOL) I-24/7 secure global communications system, as well as its array of investigative and analytical databases, and its system of Notices, within the framework of the fight against terrorism. In this regard, States should consider integrating the INTERPOL I-24/7 network into their national systems and, where appropriate, extending access to the network beyond the INTERPOL National Central Bureaus (NCBs) to other national law enforcement entities at strategic locations such as remote border crossings, airports, customs and immigration posts, or police stations.

Based on information gathered in the context of the country visits undertaken on behalf of the Counter-Terrorism Committee, as well as through direct dialogue with Member States, CTED is able to recommend ways to address the identified gaps and challenges and facilitate delivery of the technical assistance required to strengthen terrorism-related law enforcement procedures and cooperation. Effective inter-agency cooperation and information-sharing at the national level is critical to ensuring that States are also able to cooperate across borders in a comprehensive and coherent manner. CTED therefore also promotes the establishment of national coordination mechanisms that engage all relevant national authorities and, where appropriate, non-governmental actors.

ADDITIONAL RESOURCES

- CTED Analytical Brief: Responding to terrorist threats against soft targets
- CTED Trends Report: Physical Protection of Critical Infrastructure Against Terrorist Attacks
- CTED Trends Alert: Greater Efforts Needed to Address The Potential Risks Posed By Terrorist Use of Unmanned Aircraft Systems
- Global Counterterrorism Forum Counterterrorism Watchlisting Toolkit

In order to keep pace with the terrorist threat, States are increasingly integrating intelligence into law enforcement operations. There is a need to develop effective mechanisms, where appropriate, for downgrading, for official use, intelligence threat data on FTFs and individual terrorists, appropriately provide such information to frontline screeners, and appropriately share such information with other concerned States and relevant international organizations. This timely sharing of and access to threat data is especially important to ensure early warning and prevent the commission of terrorist acts.

Watch lists or databases are national or regional alert systems that provide advance warnings and checking procedures to assist in the recognition and identification of suspected criminals, terrorists and suspicious goods or materials at border-crossing points or in the early detection of suspected or previously unknown criminals and terrorists. To facilitate international information-sharing, it is essential that States develop, establish and maintain appropriate national watch lists and databases and ensure that all competent national authorities have access to them. States are encouraged to ensure the interoperability of their national watch lists and databases and to establish connectivity with regional and international watch lists and databases and enable information-sharing, as appropriate, with relevant competent authorities, whether nationally or internationally. In its resolution 2396 (2017), the Security Council decided that States should develop watch lists or databases of known and suspected terrorists, including FTFs, for use by law enforcement, border security, customs, military and intelligence agencies, to screen travellers and conduct risk assessments and investigations, in compliance with domestic and international law, including human rights law. The Council encouraged States to share that information through bilateral and multilateral mechanisms, in compliance with domestic and international human rights law.

In order to bring terrorists to justice, law enforcement agencies must be able to conduct criminal investigations in a manner that enables the prosecution to bring the case before a court. This requires a professional investigative capacity, as well as close cooperation between investigators and prosecutors. CTED promotes such cooperation by identifying investigating bodies' technical assistance needs in areas such as crime-scene management, forensic analysis, the collection of evidence, and overall analytical capacity. CTED also works to identify emerging terrorist trends to help law enforcement agencies develop effective operational countermeasures and strategies.

Terrorist attacks against critical infrastructure represent a major security threat to States of all regions. Security Council resolution 2341 (2017) calls upon States to address the danger of terrorist attacks against critical infrastructure and invites States to consider possible preventive measures in developing national strategies and policies. Physical-protection measures can reduce the risk of high-impact terrorist attacks against, inter alia, airports, seaports, railway stations, dams, nuclear power plants, chemical plants, and communications and financial systems. The *Compendium of good practices on the protection of critical infrastructure against terrorist attacks,*[1] launched in 2018, provides reference materials and guidance on the development and strengthening of risk-reduction strategies, focusing on, inter alia, prevention, preparedness, mitigation, investigation, response, recovery and other relevant concepts in the protection of critical infrastructure.

In its resolution 2396 (2017), the Security Council stresses the need for States to develop, review, or amend national risk and threat assessments to take into account "soft" targets, in order to develop appropriate contingency and emergency-response plans for terrorist attacks. It also calls on States to establish or strengthen national, regional and international partnerships with public and private stakeholders and to share information and experiences in order to prevent, protect, mitigate, investigate, respond to, and recover from damage from terrorist attacks against "soft" targets. "Soft" targets are attractive to terrorists, including FTFs, because they are relatively open and easy to access; are subject to lower levels of security protection; and offer an opportunity not only to cause massive destruction, high civilian casualties, and widespread publicity with limited financial resources, but also to instil fear into the public. Such attacks have increased in numbers in every region of the world over recent years.

The effective protection of critical infrastructure and "soft" targets requires not only the implementation of physical-protection measures, but also the development of multi-layered approaches (including response, recovery, and investigations) to such attacks and the development of strong and resilient communities and close engagement with civil society and local leadership, including religious leaders. CTED has identified the need for States to develop or expand existing national strategies and action plans to consider the risk and threat to critical infrastructure and "soft" targets. This includes identifying, prioritizing, and protecting such targets. Preparedness efforts should also include mechanisms to promote risk-based decision-making, information-sharing, and the development of public-private partnerships to counter terrorist attacks, and specifically terrorist attacks against critical infrastructure and "soft" targets.

Global concern at the risks and threats posed by the use of UAS for terrorist purposes has grown rapidly in recent years. The potential threat that the use of weaponized UAS for terrorist purposes could pose has also increased the need to adopt legislation to regulate their use, keep pace with technological developments in this area, and develop detection and counter-UAS mechanisms. It should also be noted that UAS offer new opportunities for law enforcement (e.g., as part of rapid-response operations or to secure an area during major public events). For States with porous borders, UAS can also serve as a cost-effective operational tool for border-management and early- warning activities.

All measures to counter terrorism, including in the field of law enforcement and information sharing, must be taken in accordance with domestic law and international obligations and in full respect for human rights and fundamental freedoms. All efforts related to law enforcement should be comprehensive, human rights-compliant, non-discriminatory and include gender- and age-sensitive perspectives.

The *Addendum to the guiding principles on foreign terrorist fighters (2018)* (S/2018/1177) provides further elements for States to strengthen their implementation of measures on developing watch lists and databases and on protecting critical infrastructure, vulnerable or "soft" targets, and tourism sites.

[1] Developed by the Global Counter-Terrorism Coordination Compact Working Group on Emerging threats and Protection of Critical Infrastructure, chaired by INTERPOL.