United Nations S/2019/998

Security Council

Distr.: General
27 December 2019

Original: English

Letter dated 27 December 2019 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council

On behalf of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism, I have the honour to submit to the Council the updated "Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions".

In accordance with Security Council resolutions 1373 (2001), 1535 (2004), 1624 (2005), 2178 (2014), 2395 (2017) and 2396 (2017), the Committee requested the Counter-Terrorism Committee Executive Directorate to update its 2017 technical guide to reflect the relevant provisions of those resolutions, as well as additional elements contained in relevant Council resolutions adopted since 2017. The updated technical guide is intended to assist the Counter-Terrorism Committee Executive Directorate and Member States within the framework of the country assessments prepared by the Directorate on behalf of the Committee.

The Committee would be grateful if the present letter and its annex could be brought to the attention of the members of the Council and circulated as a document of the Council.

(*Signed*) Luis F. **Ugarelli**
Chair
Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism

Annex

Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions

Contents

I. Introduction

1. In accordance with Security Council resolutions 1373 (2001), 1535 (2004), 1624 (2005), 2178 (2014), 2395 (2017) and 2396 (2017), the Counter-Terrorism Committee Executive Directorate is required to assist the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism (Counter-Terrorism Committee) to monitor, facilitate and promote the implementation by Member States of Council resolutions 1373 (2001), 1624 (2005), 2178 (2014) and 2396 (2017). In this regard, the Committee has requested the Directorate to update its technical guide[1] to reflect the requirements of the relevant successor resolutions to resolution 1373 (2001). The guide is intended as a reference tool to help to ensure consistent analysis of States' implementation efforts.

2. The guide addresses individual paragraphs of resolutions 1373 (2001) and 1624 (2005) and identifies critical provisions of resolutions 2178 (2014) and 2396 (2017). The guide also takes into account the requirements set forth in resolutions 2129 (2013), 2133 (2014), 2178 (2014), 2195 (2014), 2220 (2015), 2242 (2015), 2253 (2015), 2309 (2016), 2322 (2016), 2331 (2016), 2341 (2017), 2347 (2017), 2354 (2017), 2368 (2017), 2370 (2017), 2379 (2017), 2388 (2017), 2462 (2019), 2467 (2019) and 2482 (2019) in order to reflect the additional elements prescribed in these resolutions. The guide also draws on the guidance set forth in the Counter-Terrorism Committee's Guiding principles on foreign terrorist fighters, also known as the Madrid Guiding Principles (S/2015/939, annex II) and the addendum to the guiding principles on foreign terrorist fighters (2018) (addendum to the Madrid Guiding Principles) (S/2018/1177, annex).

3. The guide was prepared by the Counter-Terrorism Committee Executive Directorate and does not impose any obligations upon States apart from those that already exist by virtue of the relevant Council resolutions and decisions, international treaties, customary international law or other voluntarily undertaken obligations. The discussion on the international counter-terrorism treaties is not aimed at establishing when States parties are or are not fulfilling their obligations under the treaties. It addresses those aspects of international law, in particular international human rights, refugee and humanitarian law, that are relevant to the implementation of the relevant Council resolutions.

4. The guide addresses the requirements of the Council relating to the work of the Counter-Terrorism Committee and the Counter-Terrorism Committee Executive Directorate in the following areas:

(a) Comprehensive and integrated counter-terrorism strategies;

(b) Countering the financing of terrorism;

(c) Border security and arms trafficking;

(d) Law enforcement and information-sharing;

(e) General legal issues, including legislation, criminal justice and international cooperation;

(f) International human rights, refugee and humanitarian law aspects of counter-terrorism in the context of resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2396 (2017) and 2462 (2019);

(g) Prohibiting and preventing incitement and recruitment to commit terrorist acts, consistent with international law, and countering violent extremism and terrorist

[1] The present technical guide was first issued in 2009 and most recently updated in 2017.

narratives, in accordance with resolutions 1624 (2005), 2178 (2014), 2354 (2017) and 2396 (2017).

5. The guide also reflects the ongoing work of the United Nations to strengthen efforts to integrate the gender dimension into peace and security operations, including counter-terrorism, as highlighted in resolutions 2122 (2013), 2195 (2014), 2242 (2015), 2331 (2016), 2354 (2017), 2395 (2017), 2396 (2017) and 2467 (2019). Good practices in integrating the gender dimension into security operations, including peacekeeping, are also considered, where relevant to the mandate of the Counter-Terrorism Committee Executive Directorate.

6. Pursuant to paragraph 29 of resolution 2395 (2017), the present guide reflects the efforts undertaken by the Directorate to integrate the impact of terrorism on children and children's rights into its work, as appropriate, including with respect to issues related to the families of returning and relocating foreign terrorist fighters. In this regard, the guide provides guidance for ensuring that measures to counter terrorism take into account the best interests of the child in a manner consistent with international law.[2]

II. General framework for each area

A. Comprehensive and integrated counter-terrorism strategies

7. In its resolution 2395 (2017), the Council encourages Member States to consider developing comprehensive and integrated national counter-terrorism strategies and effective mechanisms to implement them that include attention to the conditions conducive to terrorism, in accordance with their obligations under international law, and encourages further the Counter-Terrorism Committee Executive Directorate to, inter alia, cooperate with Member States and international, regional and subregional organizations, and other relevant partners, upon request, to assess and advise on formulating such strategies and the mechanisms to implement them.

8. Pursuant to paragraph 6 of resolution 1963 (2010) and paragraph 18 of resolution 2129 (2013), the Counter-Terrorism Committee Executive Directorate is encouraged to engage in a dialogue with Member States aimed at advising them, as appropriate, on the development of comprehensive and integrated national counter-terrorism strategies and the mechanisms to implement them that include attention to the factors that lead to terrorist activities. Terrorists are increasingly able to bypass law enforcement measures and employ other methods, such as recruitment through the Internet and social media. This poses significant challenges to law enforcement and increases the overall threat.

9. States are therefore encouraged to consider, as part of their national strategies, measures to strengthen the resilience of the population through a balanced, multidisciplinary and holistic approach that integrates law enforcement measures and measures to address the socioeconomic, political, educational, developmental, human rights, gender and rule-of-law dimensions.

B. Countering the financing of terrorism

10. Resolutions 1373 (2001), 2178 (2014), 2253 (2015), 2368 (2017), 2396 (2017) and 2462 (2019) require States to criminalize the financing of terrorism and to take a

[2] Resolutions 2242 (2015) and 2396 (2017); and addendum to the Madrid Guiding Principles, para. 8.

number of measures to prevent and suppress it. Resolution 2341 (2017) contains additional provisions on the financing of a terrorist attack intended to destroy or disable critical infrastructure.

11. Resolution 2331 (2016) addresses the issue of trafficking in persons committed with the purpose of supporting terrorist organizations or individual terrorists, including through the financing of and recruitment for the commission of terrorist acts. In its resolution 2388 (2017), the Council calls upon Member States to increase their capacity to conduct proactive financial investigations to track and disrupt human trafficking and identify potential linkages with terrorism financing.

12. In its resolution 2396 (2017), the Council calls upon Member States to intensify and accelerate the timely exchange of relevant operational information and financial intelligence regarding actions or movements, and patterns of movements, of terrorists or terrorist networks, including foreign terrorist fighters and their families. This call is also reiterated in resolutions 2462 (2019) and 2482 (2019). Resolution 2462 (2019) is the first Council resolution devoted to preventing and suppressing the financing of terrorism. The resolution brings a new focus on terrorism-financing risks, urging all States to assess their respective risks. It is also notable for its recognition of the value of financial intelligence in counter-terrorism, including in detecting networks of terrorists and their financiers. In the resolution, the Council demands that, in implementing the provisions of the resolution, Member States comply with their obligations under international law, including international humanitarian law, international human rights law and international refugee law.

13. Analysis of Member States' implementation of those measures is guided by the provisions of the relevant United Nations conventions and by relevant international instruments, standards and good practices of the relevant international and regional bodies, in particular the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation of the Financial Action Task Force, as revised in February 2012, including recommendation 5 (Terrorist financing offence), recommendation 6 (Targeted financial sanctions related to terrorism and terrorist financing) and the related guidance.

14. In its resolution 1617 (2005), the Council strongly urges all Member States to implement the recommendations of the Financial Action Task Force. The Task Force methodology focuses on assessing the effectiveness of measures through the evaluation of the implementation of immediate outcomes.[3] The Task Force regularly updates the recommendations and methodology to reflect new threats or vulnerabilities. The Council has urged Member States to implement the recommendations in a number of subsequent resolutions, including resolutions 2253 (2015), 2368 (2017), 2395 (2017) and 2462 (2019).

C. Border security and arms trafficking

15. The obligations related to border security set forth in resolution 1373 (2001) require action in a number of areas, including immigration and customs control and aviation, maritime and cargo security. In the resolution, the Council also calls upon all States to take the necessary steps to prevent the commission of terrorist acts; to intensify and accelerate the exchange of operational information; to cooperate in preventing trafficking in arms, explosives and sensitive materials; and to ensure that asylum and refugee procedures are not abused by persons involved in terrorist acts. Effective border management is of particular importance with respect to foreign

[3] For more information on the immediate outcomes, see the *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems*.

terrorist fighters, as reflected in resolution 2178 (2014) and subsequently reaffirmed in resolution 2396 (2017), which includes requirements for Member States to establish advance passenger information systems and develop the capability to collect, process and analyse passenger name record data.

16. The instruments, standards and other practices proposed in the present guide should be used in the assessment of Member States' implementation efforts. Border security includes controls on the movement of people (immigration) and goods (customs) across borders, as well as the prevention of unlawful interference in civil aviation, maritime navigation and international cargo movement. In most of these areas, international instruments and standards have been developed by specialized international organizations, such as the International Civil Aviation Organization (ICAO), the International Maritime Organization (IMO) and the World Customs Organization.

17. The principal sources of international standards relating to the prevention of trafficking in small arms and light weapons are the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime (Firearms Protocol); the International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons; the United Nations Office on Drugs and Crime (UNODC) legislative guide for the implementation of the Firearms Protocol; the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects; and other references developed by the United Nations Development Programme, the Office for Disarmament Affairs of the United Nations and the United Nations Institute for Disarmament Research.

D. Law enforcement and information-sharing

18. There are no internationally agreed standards for law enforcement in the field of counter-terrorism. However, United Nations bodies have adopted numerous "soft law" instruments governing the conduct of law enforcement bodies and the treatment of individuals who come into contact with them. In most States, law enforcement authorities have the primary responsibility for countering terrorism. They are therefore key to the effective implementation of Council resolutions on terrorism.

19. Police forces are increasingly taking part in efforts to prevent terrorism. In its resolution 2322 (2016), the Council calls upon States to continue sharing information on the ongoing international counter-terrorism cooperation, including among special services, security agencies and law enforcement organizations and criminal justice authorities. In its resolution 2341 (2017), the Council calls upon Member States to explore ways to exchange relevant information and to cooperate actively in the prevention, protection, mitigation, preparedness, investigation, response to, or recovery from, terrorist attacks planned or committed against critical infrastructure. In addition, in its resolution 2396 (2017), the Council calls upon States to establish partnerships with stakeholders and to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks against "soft" targets. Critical infrastructures and "soft" targets are especially vulnerable to terrorist attacks and have rapidly become terrorists' preferred targets. In paragraph 15 (b) of resolution 2482 (2019), the Council calls upon Member States to consider establishing, in conformity with international law, appropriate laws and mechanisms that allow for the broadest possible international cooperation, including the appointment of liaison officers, police-to-police cooperation, the creation/use of joint investigation mechanisms, and enhanced coordination of

cross-border investigations in cases related to the linkages between terrorism and organized crime, whether domestic or transnational.

20. In its resolution 2396 (2017), the Council decides that Member States shall develop watch lists or databases of known and suspected terrorists, including foreign terrorist fighters, 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. In addition, Member States are encouraged to share this information through bilateral and multilateral mechanisms.

21. Law enforcement plays a role in several other areas covered by the present guide, which refers in this regard to the Counter-Terrorism Committee's Madrid Guiding Principles and the addendum to the Madrid Guiding Principles, as well as to actions encouraged by other relevant international instruments, standards and good practices, including the relevant memorandums of understanding of the joint United Nations Counter-Terrorism Centre/Counter-Terrorism Implementation Task Force[4]/ Global Counterterrorism Forum document entitled "Good practices in the area of border security and management in the context of counterterrorism and stemming the flow of 'foreign terrorist fighters'", the International Criminal Police Organization (INTERPOL) guidelines on combating terrorism and on integrated border management and the standards concerning the provision of round-the-clock support to policing and law enforcement services provided by the INTERPOL General Secretariat to its member States through the INTERPOL National Central Bureaus, as well as the practices of the European Police Office (Europol) Police Working Group on Terrorism and other regional police associations, the Code of Conduct for Law Enforcement Officials (General Assembly resolution 34/169, annex) and the Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (adopted in Havana in 1990).

E. General legal issues, including legislation, criminal justice and international cooperation

22. In its resolutions 1373 (2001) and 2178 (2014), the Council imposes legal obligations on Member States in a number of areas and calls upon States to take additional measures related to their general legal frameworks, including codification of the international counter-terrorism instruments, denial of safe haven, recruitment, jurisdiction, bringing terrorists to justice and international legal cooperation.

23. The Council also calls upon States to identify existing good practices among international, regional and subregional organizations (including practices developed by UNODC in its model legislative provisions against terrorism). The provisions of the 19 international counter-terrorism instruments and additional amendments also set forth specific measures relating to codification, investigation, prosecution, adjudication, jurisdiction, international cooperation and denial of safe haven. In addition, many provisions contained in the terrorism-related conventions and protocols expressly require compliance with various aspects of international human rights, refugee and humanitarian law, including the right to fair treatment, and the rule of law. These measures will, if comprehensively introduced, enhance the implementation of resolutions 1373 (2001), 1624 (2005), 2178 (2014) and 2396 (2017).

[4] Replaced by the United Nations Global Counter-Terrorism Coordination Compact Task Force in 2019.

24. In its resolution 2322 (2016), the Council adds additional requirements aimed at strengthening international cooperation, including by investigators, prosecutors and judges, in order to prevent, investigate and prosecute terrorist acts. In paragraph 24 of resolution 2396 (2017), the Council underscores the need for Member States to strengthen international judicial cooperation, as outlined in resolution 2322 (2016) and in the light of the evolving threat of foreign terrorist fighters. Those requirements are described in the present guide. In resolution 2341 (2017), the Council calls upon Member States to explore ways to exchange relevant information and to cooperate actively in the prevention, protection, mitigation, preparedness, investigation, response to, or recovery from, terrorist attacks planned or committed against critical infrastructure. In the resolution, the Council calls upon all Member States to ensure that they have established criminal responsibility for terrorist attacks intended to destroy or disable critical infrastructure, as well as the planning of, training for, and financing of and logistical support for, such attacks. In paragraph 27 of resolution 2396 (2107), the Council calls upon Member States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks against "soft" targets.

25. In paragraph 29 of resolution 2396 (2017), the Council calls upon Member States to assess and investigate suspected individuals whom they have reasonable grounds to believe are terrorists, including suspected foreign terrorist fighters and their accompanying family members, including spouses and children, entering those Member States' territories, to develop and implement comprehensive risk assessments for those individuals and to take appropriate action, including by considering appropriate prosecution, rehabilitation and reintegration measures, and emphasizes that Member States should ensure that they take all such action in compliance with domestic and international law. In paragraphs 40 and 41, the Council encourages Member States to take all appropriate actions to maintain a safe and humane environment in prisons and to take all appropriate actions to prevent inmates who have been convicted of terrorism-related offences from radicalizing to violence other prisoners with whom they may come into contact, in compliance with domestic and international law. In paragraph 31, the Council emphasizes that women and children associated with foreign terrorist fighters returning or relocating to and from conflict may have served in many different roles, including as supporters, facilitators or perpetrators of terrorist acts, and require special focus when developing tailored prosecution, rehabilitation and reintegration strategies, and stresses the importance of assisting women and children associated with foreign terrorist fighters who may be victims of terrorism, and to do so taking into account gender and age sensitivities.

26. The present guide also addresses a number of practical and institutional issues. In paragraph 2 (e) of resolution 1373 (2001), for example, the Council requires all 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. This requirement lends itself to a review of the extent to which the related legislation is being effectively implemented by Member States. A similar approach is followed with respect to international cooperation.

F. International human rights, refugee and humanitarian law aspects of counter-terrorism in the context of resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2396 (2017) and 2462 (2019)

27. The Council has stressed that States must ensure that any measures taken to combat terrorism comply with all their obligations under international law and that

they should adopt such measures in accordance with international law, in particular international human rights, refugee and humanitarian law. The Council has directed the Counter-Terrorism Committee Executive Directorate, in accordance with its mandate, to advise the Counter-Terrorism Committee on issues relating to such law in connection with the identification and implementation of effective measures to implement resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2396 (2017) and 2462 (2019). In its policy guidance on human rights adopted in 2006, the Counter-Terrorism Committee set out its position on human rights, directing the Directorate to take relevant issues into account, including in analysing States' implementation of resolution 1373 (2001).[5]

28. In its resolutions 2178 (2014) and 2396 (2017), the Council underscores that respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures and are an essential part of a successful counter-terrorism effort, and notes the importance of respect for the rule of law so as to effectively prevent and combat terrorism, noting that the failure to comply with these and other international obligations, including under the Charter of the United Nations, is one of the factors contributing to increased radicalization to violence and fosters a sense of impunity.

29. In paragraph 6 of resolution 2462 (2019), the Council demands that Member States ensure that all measures taken to counter terrorism, including measures taken to counter the financing of terrorism as provided for in the resolution, comply with their obligations under international law, including international humanitarian law, international human rights law and international refugee law, and, in paragraph 24, it urges States, when designing and applying measures to counter the financing of terrorism, to take into account the potential effect of those measures on exclusively humanitarian activities, including medical activities, that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law.

30. The present guide has been prepared in recognition of the fact that international human rights and humanitarian law obligations undertaken by States around the world differ. Some States are not party to certain of the universal human rights or international humanitarian law instruments and many are parties to regional human rights instruments that differ in certain respects. There are also differing understandings with respect to the incorporation of international human rights and international humanitarian law standards into domestic law. Nonetheless, human rights are inherent to all human beings and are universal, interrelated, interdependent and indivisible. Moreover, certain human rights may never be suspended or restricted, including in times of public emergency or armed conflicts.[6] Non-derogable rights

[5] Counter-Terrorism Committee, "Conclusions for policy guidance regarding human rights and the Counter-Terrorism Committee: policy guidance PG.2", 25 May 2006. Available at www.un.org/sc/ctc/news/document/sac-402006pg-2-conclusions-for-policy-guidance-regarding-human-rights-and-the-ctc/.

[6] Article 4 of the International Covenant on Civil and Political Rights states that, in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, no derogation from articles 6, 7, 8 (paragraphs 1 and 2), 11, 15, 16 and 18 may be made. In its general comment No. 29 (2001) on derogations from provisions of the Covenant during a state of emergency, the Human Rights Committee recognized several examples of peremptory norms from which States can never derogate, beyond those listed in article 4 of the Covenant, including fundamental principles of fair trial (including the presumption of innocence), freedom from arbitrary deprivation of liberty and prohibition of collective punishment.

include the right to life,[7] freedom from torture,[8] freedom from enslavement or servitude[9] and freedom of thought, conscience and religion.[10] Some principles, such as the absolute prohibition of torture, are considered to have attained the status of jus cogens, meaning that they may never be subject to derogation by any State.

31. Key sources of human rights guidance include the findings of the United Nations special procedures mechanisms and the jurisprudence of United Nations treaty bodies. In implementing their obligations pursuant to the aforementioned resolutions, States must also have due regard to international refugee law, including the Convention relating to the Status of Refugees of 1951 and its Protocol relating to the Status of Refugees of 1967. Key sources of international humanitarian law are the four Geneva Conventions of 12 August 1949 and the two Additional Protocols thereto of 1977.

G. Prohibiting and preventing incitement and recruitment to commit terrorist acts, consistent with international law, and countering violent extremism and terrorist narratives in accordance with resolutions 1624 (2005), 2178 (2014), 2354 (2017) and 2396 (2017)

32. The Council, in paragraphs 1 and 3 of resolution 1624 (2005), calls upon all States to adopt such measures as may be necessary and appropriate and in accordance with their obligations under international law to prohibit by law incitement to commit a terrorist act or acts, to prevent such conduct and to counter incitement of terrorist acts motivated by extremism and intolerance. Within the framework of the country visits conducted on behalf of the Counter-Terrorism Committee and in other dialogue with Member States, the Counter-Terrorism Committee Executive Directorate has urged Member States to consider taking a comprehensive approach to the effective implementation of resolutions 1624 (2005), 2178 (2014), 2354 (2017) and 2396 (2017) through legal and law enforcement measures, as well as other relevant initiatives, to address the threat of incitement to commit terrorist acts. In paragraph 16 of resolution 2178 (2014), the Council encourages Member States to engage relevant local communities and non-governmental actors in developing strategies to counter the violent extremist narrative that can incite terrorist acts, address conditions conducive to the spread of violent extremism, which can be conducive to terrorism, including by empowering youth, families, women, religious, cultural and education leaders and all other concerned groups of civil society, and adopt tailored approaches to countering recruitment and promoting social inclusion and cohesion. Initiatives to counter violent extremism may include the establishment of interreligious and intercultural dialogue mechanisms, educational and religious initiatives and community engagement programmes, or the development of national strategies to counter violent extremism.

33. In its resolutions 2354 (2017) and 2396 (2017), the Council urges Member States to implement the comprehensive international framework to counter terrorist narratives that was submitted by the Counter-Terrorism Committee to the Council in April 2017 (S/2017/375, annex), with recommended guidelines and good practices to effectively counter the ways that Islamic State in Iraq and the Levant (ISIL, also known as Da'esh), Al-Qaida and associated individuals, groups, undertakings and

[7] Universal Declaration of Human Rights, art. 3; and International Covenant on Civil and Political Rights, art. 6.

[8] Universal Declaration of Human Rights, art. 5; and International Covenant on Civil and Political Rights, arts. 7 and 4 (2).

[9] Universal Declaration of Human Rights, art. 4; and International Covenant on Civil and Political Rights, arts. 8 and 4 (2).

[10] Universal Declaration of Human Rights, art. 18; and International Covenant on Civil and Political Rights, arts. 18 and 4 (2).

entities use their narratives to encourage, motivate and recruit others to commit terrorist acts.

34. In its resolution 2396 (2017), the Council underlines the importance of strengthening international cooperation to address the threat posed by foreign terrorist fighters, including on preventing and countering incitement to commit terrorist acts, preventing radicalization to terrorism and the recruitment of foreign terrorist fighters.

35. In paragraph 38 of the same resolution, the Council calls upon States to develop and implement risk assessment tools to identify individuals who demonstrate signs of radicalization to violence and to develop intervention programmes, including with a gender perspective, in compliance with applicable international and domestic law and without resorting to profiling based on any discriminatory grounds prohibited by international law.

Chapter I. Security Council resolution 1373 (2001), paragraph 1

36. In paragraph 1 of resolution 1373 (2001), the Security Council decides that all States shall:

(a) Prevent and suppress the financing of terrorist acts;

(b) Criminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds be used, or in the knowledge that they are to be used, in order to carry out terrorist acts;

(c) Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;

(d) Prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons.

A. Criminalizing the financing of terrorism

37. The financing of terrorism should be both a predicate offence to money-laundering and a stand-alone offence. Offences such as aiding and abetting are not adequate substitutes.

38. The scope of the offence, as set forth in article 2 of the International Convention for the Suppression of the Financing of Terrorism of 1999, is worth noting. It refers to the terrorist acts criminalized under not only all the offences set forth in the various counter-terrorism instruments mentioned in the Convention, but also to the generic offence. Thus, the offence of financing terrorism should also apply in relation to the 15 offences contained in the 19 international counter-terrorism instruments. Intent and purpose are required for the generic acts, but not for the acts criminalized under the Convention and other universal instruments. Legal frameworks that cover only the self-contained “generic” definition of terrorist acts are unlikely to capture fully the offences set forth in treaties. Analysts should ascertain whether a State has criminalized both the financing of the acts described in the treaties (to the extent that such State is a party to the treaties) and the financing of acts as defined in paragraph 5 of resolution 2462 (2019) and paragraph 2 of the interpretive note to Financial Action Task Force recommendation 5.

39. Recommendation 5 of the Financial Action Task Force and its interpretive note go beyond the obligations contained in the International Convention for the Suppression of the Financing of Terrorism in requiring States to also criminalize the financing of terrorist organizations and individual terrorists on a broader basis without requiring a link to a specific terrorist act or acts. This obligation is reaffirmed in paragraph 17 of resolution 2253 (2015) and in paragraph 18 of resolution 2368 (2017), in which the Council highlights that recommendation 5 applies to the financing of terrorist organizations or individual terrorists for any purpose, including,

but not limited to, recruitment, training, or travel, even in the absence of a link to a specific terrorist act. In paragraph 5 of resolution 2462 (2019), the Council decides that the wilful financing of terrorist organizations and individual terrorists for any purpose shall be established as a criminal offence, even in the absence of a link to a specific terrorist act. The Task Force has published detailed guidance[11] on the criminalization of terrorism financing in accordance with its recommendation, which examines how both United Nations and Task Force requirements can be implemented in the context of different legal traditions, including all the elements set out below.

40. Terrorism-financing offences should extend to any funds, whether deriving from a legitimate or illegitimate source. A definition of funds should be included in the law or in the criminal code and should comply with the definition contained in the International Convention for the Suppression of the Financing of Terrorism. The definition of "funds" must be broad and must include assets that may potentially be used to obtain goods and services, as well as trade resources. In October 2016, the Financial Action Task Force revised the interpretive note to recommendation 5. The revisions included replacing the term "funds" with the expression "funds or other assets" in order to explicitly cover the provision of "economic resources" (namely, oil, oil products, modular refineries and related material, and other natural resources) in accordance with resolutions 2161 (2014), 2199 (2015) and 2253 (2015). This requirement is reaffirmed in resolutions 2368 (2017) and 2462 (2019).

41. Terrorism-financing offences should not require that the funds: (a) were actually used to carry out or attempt to carry out a terrorist act or acts; or (b) be linked to a specific terrorist act or acts.

42. The person providing or collecting the funds should have the knowledge or the unlawful intention that the funds are to be provided to a terrorist organization or an individual terrorist for any purpose. It is not necessary, however, that the financier have any specific knowledge of how these funds ought to be used or are intended to be used.

43. States should ensure that the intent and knowledge required to prove the terrorism-financing offence may be inferred from objective factual circumstances.

44. States shall establish as a criminal offence the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds be used, or in the knowledge that they are to be used, in order to finance the travel of individuals who travel to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.[12]

45. In order to supplement an incomplete criminal offence of terrorism financing, in particular with regard to the financing of a terrorist organization or individual terrorist, some States have used the offence of breaching asset-freezing requirements. It is required, in this case, that the prohibition from making funds, financial assets or economic resources or other related services available, directly or indirectly, to terrorist organizations or individual terrorists, when committed wilfully for any purpose, even in the absence of a link to a specific terrorist act (as set forth in paragraph 1 (d) of resolution 1373 (2001)), is made a criminal offence. This position is reaffirmed in paragraph 20 of resolution 2253 (2015) and in paragraph 21 of resolution 2368 (2017).

[11] Financial Action Task Force, "FATF guidance: criminalising terrorist financing (recommendation 5)", Paris, October 2016.

[12] Resolution 2178 (2014), para. 6 (b).

46. Criminalization should be in accordance with article 6 of the International Convention for the Suppression of the Financing of Terrorism, that is to say, criminal acts cannot be justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.

47. The following issues should be considered:

(a) Is the financing of terrorism criminalized as a stand-alone offence?

(b) Is every element of the offence covered?

(c) Is the collection of funds criminalized independently of the provision of funds?

(d) Is the financing of terrorism listed as a predicate offence to the money-laundering offence?

(e) Does the definition of "funds" provided for in domestic law cover any funds, whether deriving from a legitimate or illegitimate source?[13]

(f) Is the definition of "funds" inclusive? Does it cover the provision of economic resources as set forth in resolutions 2161 (2014), 2199 (2015), 2253 (2015), 2368 (2017) and 2462 (2019) and in accordance with recommendation 5 of the Financial Action Task Force and its interpretive note?

(g) Does the "terrorism-financing" offence in domestic law apply even in the absence of a link to a specific terrorist act?

(h) Does the "terrorism-financing" offence in domestic law cover the financing of both an individual terrorist or a terrorist organization, for any purpose?[14]

(i) Does the "terrorism-financing" offence cover the financing of all offences created pursuant to the 19 international counter-terrorism instruments?

(j) Does the "terrorism-financing" offence apply to the financing of travel to another country by a foreign terrorist fighter for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training?

(k) Does the "terrorism-financing" offence apply to financing a terrorist attack intended to destroy or disable critical infrastructure?

48. The following Financial Action Task Force recommendations should be consulted:

(a) Confiscation and provisional measures (recommendation 4);

(b) Terrorist financing offence (recommendation 5 and its interpretive note and immediate outcome 9), and Financial Action Task Force, "Guidance on criminalising terrorist financing (recommendation 5)", Paris, July 2019;

(c) Implementation of relevant international instruments (recommendations 36–39).

B. Freezing terrorists' assets without delay

49. One of the most effective ways to combat terrorism is to prevent terrorists and terrorist entities from accessing the funds necessary for recruitment, training, travel

[13] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 1.1.6.

[14] Ibid., template 1.1.7.

and the planning and commission of terrorist acts, including for the planning of, training for, and financing of and logistical support for, terrorist attacks intended to destroy or disable critical infrastructure.

50. The obligation to freeze, without delay, funds and assets linked to terrorist organizations or individual terrorists is a key element of resolution 1373 (2001). All elements of the provision set forth in paragraph 1 (c) of the resolution should be in place, and the State should be able to freeze funds, other financial assets or economic resources without delay.

51. States should have in place a legal provision that provides for the freezing of terrorist funds and assets pursuant to resolution 1373 (2001) and establish a designating mechanism with adequate due process consideration, as well as a dedicated mechanism to address foreign asset-freezing requests. The decisions to freeze funds and assets must be communicated to the private sector in order to identify and detect any funds or financial assets held by designated person or entities. Regular reviews of the designations to ensure that the persons and entities whose assets have been frozen still represent a terrorist threat to the State could be considered.[15]

52. A complementary requirement to the asset-freezing requirement is to prohibit anyone from making funds, financial assets or economic resources and other related services available to terrorists and terrorist entities, as set forth in paragraph 1 (d) of resolution 1373 (2001). Paragraph 1 (d) should be treated, together with the asset-freezing requirement set forth in paragraph 1 (c), as a prohibition. Once an individual who, or an entity which, commits, or attempts to commit, a terrorist act has been designated, providing any funds, assets, economic resources, financial or other related services to those individuals or entities should be prohibited. States are not required to criminalize breaches of this prohibition (although many do criminalize wilful breaches as either a sanctions offence or a terrorism-financing offence). Most Member States have introduced administrative or monetary fines as sanctions for anyone contravening the prohibition or for institutions failing to exercise adequate due diligence to avoid breaches.

53. In paragraph 19 of resolution 2253 (2015), the Council clarifies that the prohibition in paragraph 1 (d) of resolution 1373 (2001) should be strict and inclusive. No funds (apart from the exemptions duly authorized by the State that designates the person or entity) may be provided to a designated individual or entity even if the funds are not intended to be used for a terrorist purpose. This provision was further reinforced in paragraph 6 of resolution 2322 (2016) and reaffirmed in paragraph 20 of resolution 2368 (2017) and paragraph 3 of resolution 2462 (2019).

54. States should employ best practices in respect of guarantees of due process in their asset-freezing systems. The Council has stressed that States must ensure that any measures taken to combat terrorism comply with all their obligations under international law and should adopt such measures in accordance with international law, in particular international human rights, refugee and humanitarian law. Pursuant to article 17 of the International Convention for the Suppression of the Financing of Terrorism, any person who is taken into custody or regarding whom any other measures are taken or proceedings are carried out pursuant to the Convention shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in conformity with the law of the State in the territory of which that person is present and applicable provisions of international law, including international human rights law. Applicable law may, depending on the State's international obligations, include provisions of the International Covenant on Civil and Political Rights and the

[15] Financial Action Task Force, "International best practices on targeted financial sanctions related to terrorism and terrorist financing (recommendation 6)", Paris, June 2013, para. 31.

International Covenant on Economic, Social and Cultural Rights, as well as provisions of the Universal Declaration of Human Rights. Among other considerations, it is necessary to consider whether judicial or other remedies that are effective, independent and impartial are available to persons or entities to challenge decisions to freeze assets. In compliance with resolution 1452 (2002), persons and entities designated under resolution 1373 (2001) may request from the State partial access to funds and resources for basic and extraordinary expenses.

55. The mechanism to be established pursuant to resolution 1373 (2001) differs from the requirements set forth in resolutions 1267 (1999), 1989 (2011) and 2253 (2015), which also establish the ISIL (Da'esh) and Al-Qaida sanctions list. Asset-freezing mechanisms may be of an administrative or criminal nature, provided that the State can freeze without delay and on an ex parte basis. Many States have in recent years adopted mechanisms to identify the persons and entities whose funds and assets should be frozen without delay. However, these mechanisms have rarely been tested. This can make assessment of effectiveness difficult. In order to facilitate the processing of third-party requests for asset freezing under resolution 1373 (2001), the Counter-Terrorism Committee Executive Directorate has developed an asset-freezing contact database, which provides the following information: name of authority designated to receive terrorist asset-freezing requests from foreign jurisdictions; email address; telephone number; fax number; acceptable languages; website address, where available; and request form, if any. To facilitate requests to its members, the Financial Action Task Force maintains a handbook that lists, for each country, points of contact, procedures, legal tests, and evidential requirements for implementing asset freezing.

56. States should consider making publicly available their national or regional asset-freezing lists pursuant to resolution 1373 (2001).[16] This provision is aimed at enhancing bilateral, regional and international cooperation in countering the financing of terrorism and ensuring the effectiveness of asset-freezing mechanisms pertaining to resolution 1373 (2001) in particular. States remain sovereign in their determination as to whether to incorporate regional or other national asset-freezing lists domestically, should they meet their own designation criteria, and pursuant to their own legal and regulatory frameworks.

57. The following issues should be considered:

(a) How does the State implement the asset-freezing requirements of resolution 1373 (2001)?

(b) Does the State freeze assets without delay?

(c) Can the State freeze funds ex parte or without prior notice?[17]

(d) How does the State identify and designate the names of persons and entities whose funds and assets are to be frozen under resolution 1373 (2001)?

(e) Can involvement in human trafficking to finance terrorism be grounds for the designation of a person or entity pursuant to the asset-freezing mechanism established under resolution 1373 (2001)?

(f) Does the State have a mechanism to address third party asset-freezing requests, which differ from mutual legal assistance procedures?

[16] Resolution 2462 (2019), para. 11.

[17] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 1.2.2.

(g) How does the State provide guidance to financial institutions and other persons or entities that may be holding targeted funds or other assets?

(h) What legal provisions does the State have in place to allow a person or entity whose funds or other assets have been frozen to challenge the freezing measure before a court or other competent authority?[18]

(i) How does the State communicate to the private sector actions taken under the freezing mechanism?

(j) How does the State monitor compliance with the relevant asset-freezing requirements and impose civil, administrative or criminal sanctions for failure to comply?

(k) Are requests to unfreeze funds or other assets dealt with in a timely manner?

(l) Can funds or other assets of persons or entities inadvertently affected by a freezing mechanism be unfrozen upon verification that the person or entity is not a designated person or entity?

(m) Does the State authorize access to funds or other assets that were frozen pursuant to resolution 1373 (2001) if such access is determined to be necessary for basic expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses in accordance with resolution 1452 (2002)?

(n) How does a person or entity whose funds or other assets have been frozen challenge that measure with a view to having it reviewed by a court or other independent administrative body?

(o) Has the State used its asset-freezing mechanism to disrupt and prevent financial support to foreign terrorist fighters?[19]

(p) Has the State frozen any assets pursuant to resolution 1373 (2001)?[20]

58. The following international instruments, standards and good practices provide guidance in this area:

(a) Resolutions 1373 (2001) and 1267 (1999) and successor resolutions;

(b) Targeted financial sanctions related to terrorism and the financing of terrorism (Financial Action Task Force recommendation 6 and its interpretive note, and immediate outcome 10);

(c) Financial Action Task Force, “International best practices on targeted financial sanctions related to terrorism and terrorist financing (recommendation 6)”, Paris, June 2013. (Provides practices that could assist States in implementing the targeted financial sanctions to prevent and suppress the financing of terrorism in accordance with the relevant Council resolutions.)

C. Preventive measures to be taken by financial institutions and non-financial businesses and professions

59. The private sector, financial institutions and financial and non-financial businesses and professions can be misused for terrorism-financing purposes, but also play a pivotal role in reporting suspected terrorism financing, mapping networks of

[18] Ibid., template 1.2.7.

[19] Resolution 2178 (2014), para. 4.

[20] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 1.2.4.

associates and building financial profiles of suspected financiers, terrorists or foreign terrorist fighters. States need to determine their own terrorism-financing risks and ensure the implementation of preventive measures against the financing of terrorism accordingly. States should also ensure that the private sector, financial and non-financial businesses and professions and any other significant economic sectors are involved in the identification of the risks and that the private sector is sensitized to the risks identified.

60. The financing of terrorism is difficult to detect because it may involve small amounts of money. In consequence, it can be difficult for the private sector to determine that the money, which may be legitimate, could in fact be used by a terrorist or a terrorist entity or for terrorist purposes. In response to the threat posed by terrorist organizations such as ISIL (Da'esh), private and public partnerships should be strengthened and adequate terrorism-financing risk indicators made available to the private sector.[21]

61. In its resolution 2462 (2019), the Council calls upon all States to enhance the traceability and transparency of financial transactions.

62. International instruments and standards on customer due diligence, the reporting obligations that arise from them, and the penalties attached to non-compliance, are exhaustive. They arise from the need for financial institutions and other businesses and professions to ensure that they can identify their customers and their customers' activities, keep relevant records and report any activity (even in the case of attempted transactions) that gives grounds for suspicion.

63. States should have in place the necessary regulatory and inspection capacity to adequately supervise reporting entities in order to ensure that effective measures are in place to prevent the raising and moving of funds through the private sector.

64. The following issues should be considered:

(a) What sectors are at risk of financing terrorism? Have risk indicators been disseminated to the private sector?

(b) Does the State impose a legal obligation on all financial institutions and designated non-financial businesses and professions to identify their customers, including beneficial owners, and keep records?

(c) Does the State impose an explicit and direct obligation to report suspicious activity related to the financing of terrorism and money-laundering?

(d) Does the State impose a reporting obligation on (i) financial institutions and (ii) designated non-financial businesses and professions? (Check each designated non-financial business and profession listed by the Financial Action Task Force.)

(e) What sanctions for breach of compliance targeted at reporting entities are provided for? Are they effective, proportionate and dissuasive?

(f) Has the State established an authority responsible for regulating and supervising reporting entities' compliance with their obligations to counter the financing of terrorism?

(g) What mechanisms for public and private sector information-sharing on terrorism financing has the State put in place?

65. The following international instruments, standards and good practices provide guidance in this area:

[21] Resolution 2253 (2015), para. 24.

(a) Assessing risks and applying a risk-based approach (Financial Action Task Force recommendation 1 and its interpretive note, and immediate outcome 1);

(b) Customer due diligence and record-keeping (Financial Action Task Force recommendations 10–12, 16, 17, 19, 22 and 23 and immediate outcome 4);

(c) Reporting of suspicious transactions, tipping-off and confidentiality (Financial Action Task Force recommendations 20 and 21 and immediate outcome 4);

(d) Internal controls (Financial Action Task Force recommendation 18 and its interpretive note, as revised in November 2017);

(e) Monitoring transactions (Financial Action Task Force recommendation 11);

(f) Transparency and beneficial ownership of legal persons and arrangements (Financial Action Task Force recommendations 24 and 25 and immediate outcome 5);

(g) Regulation and supervision (Financial Action Task Force recommendations 26–28 and immediate outcome 3);

(h) Financial Action Task Force, "Guidance on private sector information sharing", Paris, November 2017.

D. Terrorism-financing risk assessments

66. States should have a clear understanding of the terrorism-financing risks to which they are exposed, as well as of the economic sectors most vulnerable to the financing of terrorism, including non-financial services (such as the construction, commodities and pharmaceutical sectors).[22]

67. National terrorism-financing risk assessments should be produced and regularly updated. States should also consider and assess risks associated with specific products and payment methods, including the use of cash and bearer negotiable instruments, virtual assets and new financial instruments.[23]

68. States should have in place specific measures to address the risk that terrorists may benefit from the financial proceeds of transnational organized crime and gain support from transnational organized criminal groups and should have the ability to prosecute terrorists benefiting from transnational organized crime and transnational organized criminals working with them. States shall conduct research and collect information to enhance knowledge and better understand the nature and scope of the linkages that may exist between terrorism and organized crime.[24]

69. The following issues should be considered:

(a) Has the State conducted a dedicated terrorism-financing national risk assessment? Has the State been involved in a regional terrorism-financing risk assessment?

(b) Does the State (including all relevant authorities) understand its risk of financing terrorism?

(c) Have financial and non-financial businesses and professions, as well as any significant economic sectors, conducted sectoral terrorism-financing risk assessments?[25]

[22] Resolution 2462 (2019), para. 14.
[23] Ibid., para. 20 (c) and (d).
[24] Resolution 2482 (2019), para. 2.
[25] For risks associated with the non-profit organization sector, see chap. I, sect. J, "Non-profit organizations".

(d) How has the terrorism-financing risk assessment been incorporated into the national counter-terrorism strategy (including its anti-money-laundering/counter-financing of terrorism strategy)?

(e) Are the competent authorities able to address the potential risks associated with the use of virtual assets and other anonymous means of monetary or financial transactions and to anticipate and address, as appropriate, the risk that new financial instruments may be abused for terrorism-financing purposes?

(f) Does the State conduct research and collect information to enhance knowledge of, and better understand, the nature and scope of the links that may exist between terrorists and transnational organized criminals? Does it also support initiatives and domestic mechanisms to effectively identify and address the linkages between terrorism and transnational organized crime?

(g) How often has such a national risk assessment been conducted and updated?

70. The following Financial Action Task Force recommendations provide guidance in this area: Assessing risks and applying a risk-based approach (Financial Action Task Force recommendation 1 and its interpretive note, and immediate outcome 1).

71. The following additional resources on terrorism-financing risk assessments may also be useful:

(a) Australian Reporting and Analysis Centre and Indonesian Financial Transaction Reports and Analysis Center (PPATK), “Regional risk assessment on terrorism financing 2016: South-East Asia and Australia”, 2016;

(b) European Commission, “Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities”, July 2019;

(c) UNODC, *Guidance Manual for Member States on Terrorist Financing Risk Assessments* (Vienna, 2018);

(d) Financial Action Task Force, *Terrorist Financing Risk Assessment Guidance* (Paris, July 2019).

E. Institutional framework necessary for combating the financing of terrorism

72. The financial intelligence unit is an important element of an anti-money-laundering/counter-financing of terrorism regime because it is responsible for receiving, analysing and disseminating reports on suspicious transactions and activities and other relevant information regarding suspected money-laundering and terrorism financing. It is usually (but not always) a key interlocutor between the authorities and the private sector and, as such, often plays a role in providing the private sector with guidance, training and feedback.

73. The financial intelligence unit should be able to obtain additional information from reporting entities and should have timely access to the financial, administrative and law enforcement information that it requires in order to undertake its functions properly.

74. An effective financial intelligence unit can therefore serve as an important catalyst to the establishment of a dynamic anti-money-laundering/counter-financing of terrorism regime, but also of an effective counter-terrorism system. Much depends

on the relations that the financial intelligence unit is able to develop with other authorities and with the private sector. Apart from the need to ensure that it complies with the core functions detailed below, there is no single model for a financial intelligence unit. Some carry out an investigative or prosecutorial role, while others are purely administrative (or a hybrid model). Most States have established a financial intelligence unit, but the range and effectiveness of their powers vary considerably. The financial intelligence units of more than 150 States and jurisdictions have joined the Egmont Group of Financial Intelligence Units in order to provide, inter alia, a secure platform for the exchange of specific information in relation to money-laundering and the financing of terrorism.

75. States should reinforce access to information and the terrorism-financing analytical capacity of their financial intelligence units, including by developing risk indicators, together with the competent authorities.[26]

76. States that have not yet done so should develop the expertise of their financial intelligence units to analyse financial intelligence of suspected activity of organized crimes that support terrorism,[27] including cases of trafficking in persons that finance terrorism, and should work with other States to develop this capacity, as called for in paragraph 5 of resolution 2331 (2016).

77. States should have in place measures to ensure that any person who participates in the financing of terrorist acts is brought to justice and that the responsible authorities have the ability to prosecute and penalize in a manner that duly reflects the seriousness of the offence.[28]

78. States should more effectively investigate and prosecute cases of terrorism financing and apply appropriate, effective, proportionate and dissuasive criminal sanctions.[29]

79. States should ensure that designated law enforcement authorities have responsibility for terrorism-financing investigations within their national counter-financing of terrorism framework. There should be a proactive financial-investigation component in all terrorism-related investigations.[30] States should put in place terrorism-financing disruption strategies aimed at addressing the challenges involved in obtaining evidence to secure terrorism-financing convictions, including, but not limited to, considering other investigations for other criminal offences that the individual or entity may also be involved in. Moreover, when conducting investigations into the financing of terrorism, the competent authorities should be able to ask for all relevant information held by the financial intelligence unit.

80. States should increase efforts to collect, analyse and share, through appropriate channels and arrangements and consistent with international and domestic law, data relating to financial flows associated with human trafficking and the extent and nature of the financing of terrorism activities through human trafficking activities.[31]

81. The following issues should be considered:

(a) Does the State have a financial intelligence unit established in law? Is the unit operationally effective in exercising its powers?

[26] Resolution 2462 (2019), para. 16.
[27] Resolution 2482 (2019), para. 15 (d).
[28] Resolution 2178 (2014), para. 6 (b).
[29] Resolution 2462 (2019), para. 8.
[30] Ibid., paras. 7 and 8.
[31] Resolution 2388 (2017), para. 9.

(b) Is it receiving, analysing and disseminating suspicious transaction reports and other relevant information regarding suspected terrorism-financing activities, as well as fulfilling the other core functions of a financial intelligence unit?

(c) How many suspicious transaction reports have been received and processed?

(d) What level of (financial and human) resources is dedicated to the financial intelligence unit?

(e) What is the relationship between the financial intelligence unit and the reporting entities (including regarding the provision of guidance on the manner of reporting and feedback)?

(f) Does the State require financial institutions to report suspicious transactions relating to the financing of terrorism to the financial intelligence unit?[32]

(g) Does the State have legal provisions in place to protect reporting entities from liability when reporting to the financial intelligence unit?[33]

(h) Does the State prohibit reporting entities, by law, from disclosing the fact that a suspicious transaction report or other information has been submitted to the financial intelligence unit?[34]

(i) Does the law provide that the financial intelligence unit may obtain additional information from reporting entities?[35]

(j) Can the financial intelligence unit suspend suspicious transactions suspected of being related to the financing of terrorism?

(k) Is there a provision in domestic law that allows the financial intelligence unit access to financial, administrative and law enforcement information?[36]

(l) How do the financial intelligence unit and financial investigators contribute to the counter-terrorism efforts of the State?

(m) Has the financial intelligence unit participated in the development of the national counter-terrorism strategy (if any)?

(n) Has the financial intelligence unit issued any guidelines and/or risk indicators (“red flags”) to strengthen financial institutions’ capacity to identify suspicious transactions, including illicit flows deriving from human trafficking?

(o) Are there mechanisms in place for cooperation and information-sharing by the financial intelligence unit and non-governmental organizations in combating human trafficking and supporting its victims?

(p) Is there a specialized, dedicated law enforcement unit responsible for countering the financing of terrorism?

(q) Have dedicated law enforcement units responsible for investigating the financing of terrorism been provided with the human and logistical resources required to perform their duties?

(r) What measures have been put in place to prioritize investigations into the financing of terrorism?

[32] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 1.4.3.

[33] Ibid., template 1.4.4.

[34] Ibid., template 1.4.5.

[35] Ibid., template 1.4.6.

[36] Ibid., template 1.4.7.

(s) Does the State conduct systematic financial investigations in all terrorism cases?

(t) Has the State put in place terrorism-financing disruption strategies?

82. The following international instruments, standards and good practices provide guidance in this area:

(a) Financial intelligence units, and responsibilities and powers of law enforcement and investigative authorities (Financial Action Task Force recommendations 5, 29, 30, 31 and immediate outcomes 4, 6 and 9);

(b) Other forms of international cooperation (Financial Action Task Force recommendations 37 and 40 and immediate outcomes 2 and 6);

(c) Reporting of suspicious transactions (Financial Action Task Force recommendation 20 and immediate outcome 4);

(d) Power to request further information from any reporting entity on the sole basis of a foreign request (i.e., without the existence of a national suspicious transaction report as a prerequisite);

(e) Reporting of cross-border wire transfers without thresholds;

(f) Central bank accounts register (Communication from the Commission to the European Parliament and the Council on an action plan for strengthening the fight against terrorist financing, 2 February 2016);

(g) Cooperation among financial intelligence units, law enforcement agencies and intelligence services.

83. The following additional resources on effective financial intelligence units may be useful:

(a) Klaudijo Stroligo, Horst Intscher and Susan David-Crockwell, *Suspending Suspicious Transactions*, World Bank Study (World Bank, Washington D.C., 2013);

(b) Egmont Group, "Egmont Group of Financial Intelligence Units operational guidance for FIU activities and the exchange of information", revised in February 2017;

(c) Egmont Group, Principles for information exchange between financial intelligence units, October 2013.

F. Using financial intelligence for investigations and proceedings

84. In paragraph 2 (f) of resolution 1373 (2001), the Council decides that all States shall afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings.

85. The investigation and prosecution of suspected foreign terrorist fighters continues to be at times significantly challenged by the difficulty of collecting sufficient admissible evidence to secure a conviction. Generating admissible evidence and converting information and intelligence into admissible evidence against foreign terrorist fighters are complex and multifaceted tasks.

86. Some States have established a central database of bank accounts to facilitate the detection of terrorist assets, in conformity with data privacy laws. In its resolution 2462 (2019), the Council calls upon Member States to accelerate the exchange of operational information and financial intelligence, including by considering the

establishment of a mechanism by which the competent authorities can obtain relevant information, including, but not limited to, bank account information, in compliance with international law, including international human rights law.

87. Information-sharing and collaboration among government agencies, as well as between government agencies and the financial sector, significantly improve the effectiveness of investigations. Financial institutions are increasingly using intelligence analysis to detect and predict financial crime risks. The financial sector possesses a wealth of information, including data on transactions, behaviours and user identity, that can assist the competent authorities in establishing financial connections between suspects and conduct preventive or post-attack analysis. In its resolution 2462 (2019), the Council encourages competent national authorities to establish partnerships with the private sector, including financial institutions, the financial technology industry and Internet and social media companies, in particular with regard to the evolution of the trends, source and methods of the financing of terrorism. Furthermore, the Council urges Member States to establish or strengthen, at the national level, a framework allowing competent national authorities, in particular financial intelligence units, intelligence services, law enforcement agencies and prosecutorial and/or judicial authorities, to gather and share information on the financing of terrorism.

88. Member States should ensure that financial institutions, as well as designated non-financial businesses and professions, can share information for the purposes of mitigating terrorism-financing risks and supplying the competent authorities with comprehensive information on criminal schemes.[37]

89. Member States should work to intensify and accelerate the timely exchange of relevant operational information and financial intelligence regarding actions or movements, and patterns of movements, of terrorists or terrorist networks, including foreign terrorist fighters and foreign terrorist fighter returnees and relocators, in accordance with domestic and international law.[38]

90. The following issues should be considered:

(a) Does the State exchange relevant financial intelligence through national, bilateral and multilateral mechanisms, in accordance with domestic and international law?

(b) What measures has the State put in place to ensure the quality of the information shared internationally between financial intelligence units on the financing of foreign terrorist fighters, returnees and relocators, and small cells, and on the activities of terrorist fundraisers and facilitators, in all jurisdictions?[39]

(c) Are the competent authorities able to use financial intelligence shared by financial intelligence units and to obtain relevant financial information from the private sector?

(d) What measures has the State taken to enhance the integration and use of financial intelligence in terrorism cases, including through enhanced inter-agency coordination and through public and private partnerships for the collection of information?

(e) Are the competent authorities able to make effective use of financial intelligence and financial footprints as a tool to detect networks of terrorists, financiers and sympathizers?

[37] Resolution 2462 (2019), para. 20 (b).
[38] Ibid., para. 19.
[39] Addendum to the Madrid Guiding Principles, guiding principle 45 (f).

(f) Are financial institutions able to (i) share information, domestically and internationally, within the same financial group, to enhance the traceability and transparency of financial transactions for the purposes of managing money-laundering and terrorism-financing risks, (ii) ensure that the competent authorities are supplied with comprehensive information on criminal schemes and to identify and register unregulated money remitters, and (iii) assess and address the risks associated with the use of cash, unregulated remittance systems (including *hawalas*) and other financial products, including prepaid cards?

91. The following international instruments, standards and good practices provide guidance in this area:

(a) Financial Action Task Force immediate outcome 6;

(b) Financial Action Task Force, "Operational issues: financial investigations guidance", Paris, June 2012;

(c) Financial Action Task Force, "Consolidated FATF standards on information sharing", Paris, updated in November 2017;

(d) Egmont Group, "Egmont Group of Financial Intelligence Units operational guidance for FIU activities and the exchange of information", revised in February 2017;

(e) International Monetary Fund handbook on countering the financing of terrorism (to be issued).

G. Money or value transfer services, including alternative remittance systems

92. Money or value transfer services include non-bank institutions that perform money transfers or remittances, such as exchange houses. They range from large, global networks to small operators active only in specific remittance "corridors". Money or value transfer services also include alternative remittance systems, such as *hawalas*, which are traditionally associated with a money transfer mechanism that operates with ties to specific geographic regions or ethnic communities that generally operate outside formal banking channels, frequently without oversight by the authorities. This can make such regions or communities vulnerable to abuse. Money or value transfer services can provide an attractive option for individuals who want to transfer or exchange currency because providers of such services often offer lower costs and greater speed than banks or allow consumers to use their services without accounts, a particular benefit for the unbanked. They are frequently used in regions with limited or no banking services.

93. Money or value transfer service providers should: (a) be subject to monitoring for compliance with anti-money-laundering/counter-financing of terrorism policies; (b) ensure that their agents are licensed or registered by a competent authority and maintain an updated list of their agents; and (c) include their agents in their anti-money-laundering/counter-financing of terrorism programmes and monitor them for compliance with those programmes.

94. States should take action to identify natural or legal persons that provide money or value transfer services without a licence or registration and impose proportionate and dissuasive sanctions on them.

95. Money or value transfer service providers should be required to comply with all the relevant preventive and reporting requirements regarding anti-money-laundering/

counter-financing of terrorism, in particular with regard to customer due diligence, record-keeping, and reporting of suspicious transactions.

96. It is not necessary for States to make alternative remittance systems illegal, but States should have the capacity to monitor and regulate those activities.

97. The following issues should be considered:

(a) Does the State regulate and effectively supervise money or value transfer services?

(b) Are persons or legal entities that provide money or value transfer services, whether formal or informal, obliged to be licensed or registered?[40]

(c) Are persons or legal entities that provide money or value transfer services, whether formal or informal, subject to anti-money-laundering/counter-financing of terrorism obligations?[41]

(d) Does the State have the means to identify persons or legal entities that perform this service without being licensed or registered?

(e) Are persons or legal entities that illegally perform this service subject to appropriate administrative, civil or criminal sanctions?[42]

(f) Has the State conducted awareness-raising campaigns towards private sector entities regarding the terrorism-financing risks associated with alternative remittance systems?[43]

98. The following instruments, standards and good practices provide guidance in this area:

(a) Money or value transfer services (Financial Action Task Force recommendations 10–12, 14, 15, 17, 22 and 23 and interpretive notes to recommendations 10, 12, 14, 17, 22 and 23, and immediate outcome 4);

(b) Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism/Financial Action Task Force, *Money Laundering through Money Remittance and Currency Exchange Providers* (June 2010);

(c) Financial Action Task Force, *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing* (Paris, October 2013);

(d) Financial Action Task Force, *Guidance for a Risk-based Approach for Money or Value Transfer Services* (Paris, February 2016).

H. Wire transfers

99. The use of wire transfers and other instruments offered by the regular financial system can be an effective way to launder illicit proceeds or to move licit money for terrorism-financing purposes, or they can be used for the generic support of terrorist activities. Terrorist individuals usually conduct structured transactions below applicable thresholds in order to avoid reporting and record-keeping obligations.

[40] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 1.5.1.

[41] Ibid., template 1.5.2.

[42] Ibid., template 1.5.3.

[43] Ibid., template 1.5.4.

100. Financial institutions should be required to ensure that all cross-border wire transfers of $/€1,000 or more are always accompanied by required and accurate originator information and required beneficiary information. For domestic wire transfers, the information accompanying the transaction should include originator information, such as the name of the originator; the originator account number (or, in the absence of an account, a unique transaction reference number that permits traceability); and the originator's address, national identity number, customer identification number or date and place of birth.

101. Beneficiary financial institutions should be required to: (a) take reasonable measures to identify cross-border wire transfers that lack originator/beneficiary information; (b) verify the identity of the beneficiary, if it has not been previously verified, and maintain this information (in case of cross-border wire transfers of $/€1,000 or more); and (c) have risk-based policies and procedures in place to determine when to execute, reject or suspend a wire transfer lacking originator/beneficiary information, and the appropriate follow-up action.

102. The following issues should be considered:

(a) Does the State ensure that financial institutions include full and accurate originator information and full and meaningful beneficiary information in electronic fund transfers and related messages?[44]

(b) Does the State oblige financial institutions to include, throughout the payment chain, the originator and beneficiary information linked to the electronic fund transfer?[45]

(c) What measures does the State have in place for enhanced scrutiny of wire transfers without such originator/beneficiary information?

103. The following standards and good practices provide guidance in this area:

(a) Wire transfers (Financial Action Task Force recommendation 16 and its interpretive note);

(b) Egmont Group, "The benefits of FIUs' collection of cross-border wire-transfer reports", November 2016.

I. Cash couriers

104. The physical cross-border transportation of cash and bearer negotiable instruments remains widespread owing to the heavy reliance on cash in many States.

105. In paragraph 1 (a) of resolution 1373 (2001), the Council directs all States to prevent and suppress the financing of terrorist acts, and in paragraph 2 (g), the Council requires all States to prevent the movement of terrorist groups through effective border controls. The International Convention for the Suppression of the Financing of Terrorism requires States parties to consider introducing measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments.

106. States are required to implement measures to detect and monitor the physical cross-border transportation of currency and bearer negotiable instruments, fully covering both incoming and outgoing cross-border transportations of currency and bearer negotiable instruments, including through containerized cargo.

[44] Ibid., template 1.6.1.
[45] Ibid., template 1.6.2.

107. Since the physical transportation of cash or bearer negotiable instruments across international borders involves at least two States, customs and other similar border authorities clearly have a significant role to play in combating this phenomenon and in enhancing effective international cooperation. However, States' customs authorities are often more concerned about capital flight than money-laundering and the financing of terrorism and thus do not adequately gather related intelligence or cooperate with the financial intelligence unit.

108. States must have in place either a declaration or disclosure system for incoming and outgoing cross-border transportations of currency and bearer negotiable instruments. States can use either system; it is not necessary to have both. In a declaration system, all persons making a physical cross-border transportation of currency or bearer negotiable instruments of a value exceeding a preset, maximum threshold of $/€15,000 should be required to submit a truthful declaration to the designated competent authorities. In a disclosure system, travellers should be required to give a truthful answer and provide the authorities with appropriate information upon request, but are not required to make an upfront written or oral declaration.

109. States must ensure that their competent authorities have the legal power to stop or restrain currency or bearer negotiable instruments that are suspected of being related to the financing of terrorism or that are falsely declared or disclosed. They should also ensure that effective, proportionate and dissuasive sanctions can be imposed on persons who make false declarations or disclosures, and adopt measures to confiscate currency or bearer negotiable instruments related to the financing of terrorism or money-laundering. In addition, States should strengthen their capacities to develop customs risk indicators at both the "pre-arrival" and "arrival" stages, raise awareness of the requirements to declare or disclose and put in place record-keeping systems to collect, gather and share traveller information.

110. In its resolution 2462 (2019), the Council calls upon Member States to strengthen international cooperation to prevent and counter the financing of terrorism, including by enhancing cross-border cooperation among and between customs and tax authorities, as well by improving the coordination of international police and customs operations.

111. The following issues should be considered:

(a) Does the State have in place either a disclosure or declaration system, or other measures, to detect the illicit physical cross-border transportation of currency and bearer negotiable instruments?[46]

(b) Do these measures apply to incoming and outgoing physical cross-border transportation of currency and bearer negotiable instruments made by a person, through mail or in containerized cargo?

(c) If the State does have a declaration system in place, is the threshold for declaration equivalent to or below $/€15,000?[47]

(d) Do the border authorities have the legal authority to stop or restrain currency and bearer negotiable instruments suspected of being related to money-laundering or the financing of terrorism?[48]

(e) Has the State adopted measures to confiscate currency or bearer negotiable instruments related to the financing of terrorism or money-laundering?

[46] Ibid., template 1.7.1.
[47] Ibid., template 1.7.4.
[48] Ibid., template 1.7.6.

(f) Are there proportionate and dissuasive civil, administrative or criminal sanctions in place for making a false declaration or disclosure?[49]

(g) Is information that is obtained through the declaration or disclosure system shared with the financial intelligence unit? If so, what kind of information is shared with the unit?[50]

(h) Do the financial intelligence unit and the customs authorities have a formal mechanism of cooperation and information-sharing?

(i) Does the State engage in efforts to raise awareness of the requirements to declare or disclose (e.g., signage, pamphlets and forms)?[51]

(j) Does the State have in place record-keeping systems to gather and share traveller information?

(k) Do the measures put in place by the State respect the freedom of capital movements?

(l) Does the State have an enforcement capacity to prevent and detect the illegal cross-border movement of cash and bearer negotiable instruments (in terms of information and intelligence, risk analysis, targeting and inspection)?[52]

112. The following international instruments, standards and good practices provide guidance in this area:

(a) Cash couriers (Financial Action Task Force recommendation 32 and its interpretive note, and immediate outcomes 6 and 7);

(b) Confiscation and provisional measures (Financial Action Task Force recommendation 4);

(c) Financial Action Task Force, “International best practices: detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments”, Paris, February 2010;

(d) Financial Action Task Force, *Money Laundering through the Physical Transportation of Cash* (Paris, October 2015);

(e) World Customs Organization, Customs enforcement guidelines on countering money laundering and terrorist financing, 2015.

J. Non-profit organizations

113. Non-profit organizations play a vital role in the world economy.

114. Given the variety of legal forms that non-profit organizations can have, the Financial Action Task Force has adopted a functional definition of such organizations under recommendation 8 (revised in October 2016), which refers to “a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of ‘good works’”. Some non-profit organizations (among those covered by the above definition) may be vulnerable to abuse for the purpose of financing terrorism for a variety of reasons, including because: (a) non-profit organizations enjoy the public trust, have access to significant

[49] Ibid., template 1.7.7.
[50] Ibid., templates 1.7.8 and 1.7.9.
[51] Ibid., template 1.7.10.
[52] Ibid., template 1.7.11.

sources of funds and use primarily cash; and (b) some non-profit organizations operate within or near areas that are most exposed to terrorist activities.

115. Measures put in place by Member States to protect non-profit organizations from potential abuse should be tailored and in accordance with a risk-based approach. It is imperative that States implement such measures in a manner that respects their obligations under the Charter of the United Nations and international human rights law.

116. Since not all non-profit organizations are inherently high-risk, States should first understand their domestic non-profit organization sector and the terrorism financing risks facing this sector in order to identify which subsets fall within the definition provided by the Financial Action Task Force and are at higher risk of financing terrorism. Having identified those subsets, States should review the adequacy of laws and regulations related to them and work closely with the sector to determine the level of measures required to ensure its protection from abuse.

117. There is a diverse range of approaches to identifying, preventing and combating abuse of non-profit organizations for the purpose of financing terrorism. An effective approach should involve all four of the following elements: (a) sustained outreach; (b) targeted risk-based supervision or monitoring; (c) effective investigation and information gathering; and (d) effective mechanisms for international cooperation.

118. States should encourage and undertake outreach and educational programmes to raise and deepen awareness among non-profit organizations, as well as the donor community, about the potential vulnerabilities of such organizations to abuse for the purpose of financing terrorism and the risks in that regard, and the measures that the organizations can take to protect themselves against such abuse. States should work with non-profit organizations to develop and refine best practices to address terrorism financing risks and vulnerabilities in order to protect them from that abuse.

119. There should be targeted risk-based supervision or monitoring. Non-profit organizations may, for instance, be licensed and registered, issue annual financial statements on their income and expenditure, have appropriate controls in place and make publicly available relevant information about their objectives, control and management. States should put in place effective mechanisms for international cooperation (by establishing appropriate points of contact and procedures to respond to international requests for information regarding particular non-profit organizations suspected of financing terrorism or of being involved in other forms of support to terrorists).

120. States are required to identify and take effective and proportionate action against non-profit organizations that either are exploited by, or are knowingly supporting, terrorists or terrorist organizations, taking into account the specifics of the case. Countries should aim to prevent and prosecute, as appropriate, the financing of terrorism and other forms of support to terrorists. Where non-profit organizations suspected of, or implicated in, terrorism financing or the provision of other forms of support to terrorists are identified, the first priority of countries must be to investigate and halt such financing or support. Actions taken for this purpose should, to the extent reasonably possible, minimize the negative impact on innocent and legitimate beneficiaries of charitable activities. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting the financing of terrorism or the provision of other forms of support to terrorists by non-profit organizations.

121. Focused measures adopted by countries to protect non-profit organizations from abuse for the purpose of financing terrorism should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote accountability

and engender greater confidence among those organizations, across the donor community and with the general public, that charitable funds and services reach the intended legitimate beneficiaries. Systems that promote achieving a high degree of accountability, integrity and public confidence in the management and functioning of non-profit organizations are integral to ensuring that they cannot be abused to finance terrorism.

122. In its resolution 2462 (2019), the Council urges States, when designing and applying measures to counter the financing of terrorism, to take into account the potential effect of those measures on exclusively humanitarian activities, including medical activities, that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law.

123. The following issues should be considered:

(a) Has the State identified which subset(s) of non-profit organizations fall(s) within the definition of the Financial Action Task Force?

(b) Has the State conducted a risk assessment or terrorism-financing review of the subset(s) of non-profit organizations that fall(s) within the definition provided by the Task Force?

(c) Has the State reviewed the adequacy of its non-profit sector laws and regulatory framework with regard to risks associated with the financing of terrorism?[53]

(d) Does the review of the State's non-profit sector laws and regulatory framework ensure that the laws and framework respect the right of non-profit organizations to freedom of association and the legitimate role played by those organizations in the collection and distribution of funds?[54]

(e) Has the State engaged with the sector in conducting its national risk assessment?

(f) How does the State involve the non-profit organization sector in the development of risk-based targeted measures to prevent abuse for the purpose of financing terrorism?

(g) Is there a domestic regulatory agency for non-profit organizations?[55]

(h) Does the State maintain a central non-profit organization database or a similar, centralized register of information (that includes, inter alia, the name, purpose, activities and director of the organization)?[56]

(i) Are there sanctions on non-profit organizations that contravene the regulatory and supervisory framework?[57]

(j) Can the information about non-profit organizations contained in non-profit organization registers be made available to law enforcement agencies and to the financial intelligence unit?[58]

(k) Does the State have effective mechanisms in place to respond to international requests for information regarding non-profit organizations suspected of financing terrorism or of being involved in other forms of support to terrorists?

[53] Ibid., template 1.8.1.
[54] Ibid., template 1.8.2.
[55] Ibid., template 1.8.3.
[56] Ibid., template 1.8.5.
[57] Ibid., template 1.8.7.
[58] Ibid., template 1.8.8.

(l) Does the State, when designing and applying measures to counter the financing of terrorism, take into account the potential effect of those measures on exclusively humanitarian activities, including medical activities, that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law?[59]

124. The following international instruments, standards and good practices provide guidance in this area:

(a) Non-profit organizations (Financial Action Task Force recommendation 8 and its interpretive note, and immediate outcome 10);

(b) Financial Action Task Force, *Risk of Terrorist Abuse in Non-Profit Organisations* (Paris, June 2014);

(c) Financial Action Task Force, *Best Practices: Combating the Abuse of Non-Profit Organisations* (Recommendation 8) (Paris, June 2015);

(d) Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (para. 38).

K. New technologies

125. In its resolution 2253 (2015), the Council expresses concern at the increased use by terrorists and their supporters of new information and communications technologies (ICTs), in particular the Internet, to facilitate terrorist acts, and condemns their use to incite, recruit, fund or plan terrorist acts.

126. Prepaid cards, credit cards, mobile banking and Internet payment systems have been used to transfer funds online for terrorism-financing purposes.

127. Online fundraising, under the pretext of legitimate humanitarian assistance, has been abused for the purpose of financing terrorism.[60]

128. The use of crowdfunding techniques also represents an emerging terrorism-financing risk.[61] Crowdfunding is an Internet-enabled way for businesses, organizations or individuals to raise money, from donations or investments, from multiple individuals. The Council has called upon all States to enhance the traceability and transparency of financial transactions, including by assessing and addressing potential risks associated with virtual assets and crowdfunding platforms and taking steps to ensure that providers of such assets are subject to anti-money-laundering/counter-financing of terrorism obligations.

129. The Council has also recognized the role of new and emerging financial and regulatory technologies to bolster financial inclusion and to contribute to the effective implementation of anti-money-laundering/counter-financing of terrorism measures.[62]

130. Virtual assets, such as bitcoin, can be exploited by criminal groups. This technology allows for the anonymous transfer of funds internationally, which could be used to finance terrorism. Terrorist groups are actively promoting their use.[63]

131. New technologies using decentralized and distributed structures, such as blockchain-related technologies, can be used and leveraged by various parties to

[59] Resolution 2462 (2019), para. 24.
[60] Financial Action Task Force, “Emerging terrorist financing risks”, Paris, October 2015, p. 34.
[61] Ibid., p. 6.
[62] Resolution 2462 (2019), para. 20 (a).
[63] Financial Action Task Force, “Emerging terrorist financing risks”, pp. 35–36.

exchange, move, withdraw or account for various classes of assets outside classical financial networks.

132. Social networks and third-party payment or communications software are used to facilitate consumer-to-consumer payments.

133. The following issues should be considered:

(a) Has the financial intelligence unit or another national competent authority conducted a national threat assessment regarding new technologies that could be abused for the purpose of financing terrorism?

(b) Do the law enforcement authorities monitor social media trends to identify new technologies used to finance terrorism?

(c) Has the Government created public-private platforms for communication with the private sector and civil society organizations to discuss the evolving threat of new technologies regarding the financing of terrorism?

(d) Is online fundraising monitored for terrorism-financing purposes?

(e) Are prepaid cards and credit cards subject to anti-money-laundering/counter-financing of terrorism legal regimes?

(f) Are Internet payment systems subject to anti-money-laundering/counter-financing of terrorism legal regimes?

(g) Are virtual assets and exchange platforms subject to anti-money-laundering/counter-financing of terrorism legal regimes?

(h) Are current methodologies and tools used by the financial intelligence unit and regulators adapted to the emergence of decentralized new technologies?

(i) How do the authorities responsible for the implementation of asset-freezing measures deal with the issue of virtual assets?

134. The following international instruments, standards and good practices provide guidance in this area:

(a) New technologies (Financial Action Task Force recommendation 15, revised in October 2018, and immediate outcome 4);

(b) Financial Action Task Force, “Emerging terrorist financing risks”, Paris, October 2015;

(c) Financial Action Task Force, “Virtual currencies: key definitions and potential AML/CFT risks”, June 2014;

(d) Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA;

(e) Arab Convention on Combating Information Technology Offences, adopted by the League of Arab States in 2010;

(f) Financial Action Task Force, *Guidance for a Risk-based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris, June 2019);

(g) Communication from the Commission to the European Parliament and the Council on an action plan for strengthening the fight against terrorist financing, 2 February 2016;

(h) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012

of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC;

(i) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU;

(j) Asia/Pacific Group on Money Laundering/Middle East and North Africa Financial Action Task Force, “Social media and terrorism financing”, January 2019.

Chapter II. Security Council resolution 1373 (2001), paragraph 2

135. In paragraph 2 of resolution 1373 (2001), the Security Council decides that all States shall:

(a) Refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists;

(b) Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information;

(c) Deny safe haven to those who finance, plan, support or commit terrorist acts, or provide safe havens;

(d) Prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other States or their citizens;

(e) 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 and ensure that, in addition to any other measures against them, such terrorist acts are established as serious criminal offences in domestic laws and regulations and that the punishment duly reflects the seriousness of such terrorist acts;

(f) Afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings;

(g) Prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents.

A. Suppressing and preventing recruitment

136. Recruitment methods employed by terrorist organizations and individuals affiliated with terrorism have evolved in accordance with the evolution of the terrorist threat. In paragraph 2 (a) of resolution 1373 (2001), the Council decides that all States shall suppress the recruitment of members of terrorist groups. The Council expanded this requirement in its resolution 2178 (2014), deciding that Member States shall, consistent with international human rights law, international refugee law and international humanitarian law, prevent and suppress the recruiting of foreign terrorist fighters.

137. Criminalization is key to the suppression of terrorist recruitment. Pursuant to paragraph 6 of resolution 2178 (2014), all States shall ensure that their domestic laws and regulations establish serious criminal offences sufficient to provide the ability to prosecute and penalize in a manner duly reflecting the seriousness of the offence, including the wilful organization of the travel of, and acts of recruitment of, individuals who travel to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. Effective enforcement is the second step in suppression.

138. In addition to the suppression of recruitment, the Council calls upon States to prevent the recruitment of terrorists. This would normally entail the development and implementation of a broader strategy to prevent recruitment. Other counter-recruitment tools include awareness-raising strategies and outreach to various communities.

139. In its resolution 2396 (2017), the Council recognizes that the threat of returning or relocating foreign terrorist fighters includes, among others, that such individuals may further support acts or activities of ISIL (Da'esh), Al-Qaida and their cells, affiliates, splinter groups and derivative entities, including by recruiting for, or otherwise providing continued support for, such entities. In paragraph 40 of the same resolution, the Council encourages Member States to develop tools that can help to address radicalization to violence and terrorist recruitment in prisons. (This issue is covered in chapter II, section K, "Prosecution, rehabilitation and reintegration".)

140. In paragraph 18 of resolution 2482 (2019), the Council calls on Member States to increase the awareness, training and capacity of relevant practitioners in correctional systems on the linkages between terrorism and organized crime, including where perpetrators of petty crime may be exploited or recruited by terrorists. Furthermore, in paragraph 20, it encourages Member States to explore ways to impede the cooperation and transfer of skills and knowledge between terrorists and other criminals, while respecting international human rights law.

141. The following issues should be considered:

(a) Does the State have in place legislative provisions to suppress the recruitment of terrorists and foreign terrorist fighters?[64]

(b) Does the State criminalize recruitment as an autonomous offence?

(c) Does the State have in place a national strategy for the suppression of recruitment?[65]

(d) Is the implementation of the criminalization of recruitment and of the national strategy based upon the principles of necessity and proportionality? Does it exclude any form of arbitrariness or discrimination?

(e) Does the implementation of the criminalization of recruitment and of the national strategy provide full respect for the rights of individuals, including, in particular, the rights to freedom of association, freedom of expression, freedom of religion, and privacy?

(f) Does the State have in place practical (i.e., operational) measures to suppress the recruitment of terrorists?[66]

(g) Does the national strategy take into account vulnerable communities and places where people could be recruited for terrorism, including places of education or religious training and worship, and prisons?

(h) Does the State have in place a specific programme to detect and eliminate recruitment and training techniques with respect to prospective candidates for suicide missions (known as "talent spotting"), as well as the employment of special methods of psychological indoctrination at the training camps set up for that purpose?[67]

[64] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.1.2.

[65] Ibid., template 2.1.1.

[66] Ibid., template 2.1.3.

[67] Meeting of Heads of Special Services, Security Agencies and Law-Enforcement Organizations, "Best practices in countering suicide terrorism" (A/71/889-S/2017/349, annex), para. 4 (b).

(i) Does the State have an awareness-raising and outreach programme for community education, community policing[68] and the creation of partnerships with local populations to establish self-sustaining community safety and security measures?

(j) Does the State integrate considerations of gender and age into efforts aimed at suppressing recruitment?

B. Terrorist recruitment through the Internet

142. It has become relatively easy for individuals wishing to join a terrorist organization or travel to a conflict zone to make direct, anonymous contact with a terrorist recruiter.[69] In order to address this threat, there is an urgent need to strengthen national, regional and international cooperation in countering the use of the Internet and social media for terrorist purposes, in particular for the recruitment of foreign terrorist fighters.[70]

143. The vast reach of the Internet provides terrorist organizations and sympathizers with a global pool of potential recruits. States, regional organizations, the private sector and civil society should establish effective partnerships with a view to developing improved methods for monitoring and studying terrorist content transmitted over the Internet and other communications technologies and countering incitement to commit terrorist acts, utilizing it for intelligence work and referring it, where appropriate, to relevant law enforcement agencies.[71]

144. Member States should also review their legal framework aimed at blocking, filtering or removing illegal Internet content to assess whether they are addressing the threat in a manner compliant with their obligations under international law and, in particular, human rights law, including fundamental freedoms.

145. The following issues should be considered:

(a) If the legal system allows for the blocking, filtering or removal of content, what requirements and safeguards are in place?

(b) What requirements and safeguards does the legal framework set for such actions?

(c) What human rights obligations and principles are taken into account in the implementation of enforcement measures in this field?

(d) Has the State established a formal or informal public-private partnership framework with ICT firms whose mandate includes counter-terrorism for monitoring and studying terrorist content over the Internet, utilizing it for intelligence work and referring it, when appropriate, to relevant law enforcement agencies?[72]

(e) Does the national strategy for the suppression of recruitment address the use of ICT for recruitment?[73]

[68] Madrid Guiding Principles.

[69] Second report of the Counter-Terrorism Committee on the implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters (S/2015/683, annex, p. 3).

[70] Ibid., para. 16.

[71] Madrid Guiding Principles, guiding principle 13.

[72] Ibid.

[73] S/2015/683, annex, para. 16.

(f) Has the State introduced measures to address the recruitment of and trafficking in women and girls by terrorist groups, in particular through the Internet?[74]

146. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles;

(b) Addendum to the Madrid Guiding Principles, guiding principles 39 and 44;

(c) Second report of the Counter-Terrorism Committee on the implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters (S/2015/683, annex);

(d) Third report of the Counter-Terrorism Committee on the implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters (S/2015/975, annex);

(e) Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat (S/2016/501);

(f) Global survey of the implementation by Member States of Security Council resolution 1373 (2001) (S/2016/49, annex);

(g) Meeting of Heads of Special Services, Security Agencies and Law-Enforcement Organizations, "Best practices in countering suicide terrorism" (A/71/889-S/2017/349, annex), para. 4 (b) on "talent spotting".

C. Eliminating the supply of weapons to terrorists

147. In paragraph 2 (a) of resolution 1373 (2001), the Council requires States to refrain from providing any form of support to entities or persons involved in terrorist acts, including by eliminating the supply of weapons to terrorists. The diversion of weaponry is a significant problem in many parts of the world, enabling terrorist groups to considerably increase their military power.[75] An influx of foreign terrorist fighters increases the probability that weapons and ammunition will be moved across borders.[76] Diversion may occur as a result of a transfer without proper controls, an unauthorized retransfer, theft from poorly secured stockpiles, handouts to armed groups or a barter involving natural resources.

148. Eliminating terrorist access to weapons and their components has become more complex and challenging for States, owing to the evolving threat and the nature of the terrorist operational environment. In its resolution 2370 (2017), the Council acknowledges, among other things, the threat posed by the use of improvised explosive devices in many terrorist attacks around the world and the need to tackle the threat in a comprehensive manner. The impact of improvised explosive devices on civilians remains a serious concern to the international community, including their use in the perpetration of terrorist attacks on roads, against commercial premises, markets and places of worship, and at public events. The use of improvised explosive devices has become common practice. They frequently take the form of improvised mortars, projectiles, grenades and landmines that are used during hostilities in a similar fashion to their conventionally produced equivalents.[77]

[74] Resolution 2331 (2016); and S/2016/501, paras. 45–47.
[75] Report of the Secretary-General on small arms and light weapons (S/2015/289).
[76] Ibid., para. 25.
[77] Report of the Secretary-General on countering the threat posed by improvised explosive devices (A/73/156).

149. The Internet is increasingly being exploited for trade in weapons, including components and precursor materials used to build improvised explosive devices. Terrorist groups actively disseminate guidance material and share know-how on manufacturing and using improvised explosive devices. Dark web markets are attractive to terrorists because they offer almost perfect anonymity and thus enable terrorists to avoid detection. In this regard, States must improve measures to prevent terrorists and terrorist organizations from obtaining, handling, storing, using or seeking access to all types of explosives, whether military, civilian or improvised, as well as to raw materials and components that can be used to manufacture improvised explosive devices or unconventional weapons. It is critical that States conduct frequent risk and threat assessments of illegal trafficking in and movements of explosive materials and establish national law-enforcement coordinating mechanisms among the relevant agencies.

150. In its resolution 2370 (2017), the Council recognizes the need for Member States to take appropriate measures, consistent with international law, to address the illicit trafficking in small arms and light weapons, in particular to terrorists, including by enhancing, where appropriate and consistent with their domestic legal frameworks, national systems for the collection and analysis of detailed data on the illicit trafficking of such weapons to terrorists, and by putting in place, where they do not exist, adequate laws, regulations and administrative procedures to exercise effective control over the production, export, import, brokering, transit or retransfer of small arms and light weapons within their areas of jurisdiction, taking into consideration the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, in order to prevent the illicit trafficking of such weapons to terrorists. In paragraph 10 of resolution 2482 (2019), the Council urges States that have not already done so, in order to prevent terrorists from acquiring weapons, to adopt and implement the necessary legislative or other measures to establish as criminal offences under their domestic law: the illegal manufacture, possession, stockpiling and trade of all types of explosives, whether military or civilian, as well as other military or civilian materials and components that can be used to manufacture improvised explosive devices, including detonators, detonating cords and chemical components; and the trafficking in military and dual-use materials and equipment that could be used for the illegal manufacture of arms and armaments, including explosive devices. In paragraph 11 of the same resolution, the Council urges States to adopt legislative and other measures, consistent with domestic marking laws and regulations, including criminal measures, to prohibit the illegal manufacture of unmarked or inadequately marked small arms and light weapons, as well as the illicit falsification, obliteration, removal or alteration of the unique markings prescribed in the International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons (International Tracing Instrument).

1. Member States should put in place an appropriate legislative framework.

151. The following issues should be considered:

(a) With respect to production, does the State define which small arms and light weapons are subject to controls; specify the national authorities and mechanisms required for the production, acquisition, ownership and control of small arms and light weapons; require the marking of small arms and light weapons; designate licensed manufacturers; establish mechanisms for the verification of marking; and designate the national authorities responsible for verification?

(b) With respect to possession, does the State set rules and regulations governing civilian acquisition, possession, transportation, licensing of dealers, record-keeping and tracing of the various categories of small arms and light weapons,

and rules requiring the reporting of lost or stolen small arms and light weapons? Does the State ban all transfers of explosives and man-portable air defence systems and their essential components to non-State end users?

(c) With respect to brokering, has the State introduced legislation regulating the activity of brokers and sellers of small arms and light weapons and explosives, as well as arms brokering in general?

(d) With respect to import and export, does the State designate a national body to review requests to export small arms and light weapons; verify weapons shipped and the relevant documentation; and prohibit the sale and/or transfer of small arms and light weapons, components, ammunitions and explosives to any non-State actors?

(e) Does the State establish specific offences, if appropriate, to prevent the illicit reactivation of deactivated firearms, consistent with the general principles on deactivation included in article 9 of the Firearms Protocol?

(f) Does the State criminalize the illicit manufacturing of, and trafficking in, small arms and light weapons and explosives; the illicit obliteration of their markings, as well as tampering with firearm markings; and the illegal moving of small arms and light weapons, explosives and man-portable air defence systems across borders?

152. The following international instruments, standards and good practices provide guidance in this area:

(a) Security Council resolutions on arms embargoes, including the embargo imposed by the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities;

(b) Firearms Protocol;

(c) Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-traps and Other Devices as amended on 3 May 1996 (Amended Protocol II), and Protocol on Explosive Remnants of War (Protocol V);

(d) Relevant modules on legislation from the International Small Arms Control Standards developed by the Coordinating Action on Small Arms (led by the Office for Disarmament Affairs of the United Nations);

(e) International Tracing Instrument;[78]

(f) Meeting of Heads of Special Services, Security Agencies and Law-Enforcement Organizations, "Best practices in countering suicide terrorism" (A/71/889-S/2017/349, annex), para. 7;

(g) The work of the Group of Experts of the High Contracting Parties to Amended Protocol II to the Convention on Certain Conventional Weapons;

(h) Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects.

[78] See also information on additional programmes, including the International Small Arms Control Standards, available at https://www.un.org/disarmament/convarms/mosaic/.

2. Member States should have in place specific procedures as part of operational measures in order to eliminate the supply of weapons to terrorists.

153. The following issues should be considered:

(a) Has the State maintained, developed or established, and effectively implemented, national laws, regulations and administrative procedures to ensure effective control over the production, export, import and transit of small arms and light weapons, including by establishing as a criminal offence their illicit manufacture, online trade or diversion to the illicit market through corruption?

(b) Has the State provided national law enforcement authorities with mandates and resources to assist them in preventing and combating the import into, export from or transit through their territories of illicit small arms and light weapons?

(c) Has the State taken all appropriate measures to prevent the diversion of small arms and light weapons when authorizing their international transfer, taking into consideration that, in the International Tracing Instrument, small arms and light weapons are considered illicit if they are transferred without a licence or authorization issued by a competent national authority?

(d) Has the State put in place and, as needed, strengthened certification processes/end-user certificates, as well as effective legal and enforcement measures, and made every effort, in accordance with national laws and practices, without prejudice to the right of States to re-export small arms and light weapons that they have previously imported, to notify the original exporting State in accordance with their bilateral agreements before the retransfer of those weapons?

(e) Does the State have procedures in place to mark small arms and light weapons?

(f) Does the State have procedures in place to ensure the control of manufacturers and the verification of production, storage, security and transfers?

(g) Does the State ensure that weapons held by government defence and security forces are safely, securely and effectively managed and properly stored and controlled, in particular in conflict and post-conflict situations, in accordance with the provisions of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects?

(h) Does the State have procedures in place to enable the registration of brokers? Has it established mechanisms to control their activities and detect and arrest those who violate Security Council arms embargoes, including on the Internet?

(i) Does the State have procedures in place to carry out the management of stockpiles and the destruction or disposal of confiscated, seized or collected small arms and light weapons and man-portable air defence systems?

(j) Does the State have procedures in place to enable the regulation of civilian possession and the identification of the owner?

(k) Does the State have in place security measures to counter the potential threat of man-portable air defence systems targeting civil aviation?

(l) Do the national systems and procedures in place to trace lost or stolen firearms include international tracing?

(m) Do the State’s relevant national law enforcement agencies have access to the INTERPOL Illicit Arms Records and Tracing Management System databases and the INTERPOL Ballistic Information Network?

(n) Does the State have in place practical measures and controls on the illicit manufacturing of, trafficking in or alteration of firearms or the illicit obliteration of their markings?

(o) Has the State taken effective measures to prevent and combat the illicit brokering of small arms and light weapons, taking advantage of the recommendations contained in the report of the Group of Governmental Experts established pursuant to General Assembly resolution 60/81?

(p) Does the State exchange and, in accordance with States' national legal frameworks and security requirements, apply experiences, lessons learned and best practices relating to the export, import and transit control, including certification processes/end-user certificates, of small arms and light weapons?

154. The following international instruments, standards and good practices provide guidance in this area:

(a) Relevant modules on legislation from the International Small Arms Control Standards developed by the Coordinating Action on Small Arms (led by the Office for Disarmament Affairs of the United Nations);

(b) Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects;

(c) United Nations demobilization, disarmament and reintegration programmes;

(d) ICAO, *Aviation Security Manual* (Doc. 8973 – Restricted), appendix 27, which contains technical recommendations and procedures to minimize the risk of an aircraft being hit by man-portable air defence systems, and supplementary guidance material available to ICAO member States through a secure website.

3. Member States should have in place an enforcement programme for the control of arms and explosives on their territory.

155. The following issues should be considered:

(a) Does the State have in place national systems and procedures to trace lost or stolen firearms?

(b) Is the State taking measures at the national level to prevent terrorists from exploiting ICT, including darknet markets, for the building of improvised explosive devices and the trafficking in small arms and light weapons?

(c) Does the State have in place national procedures to trace illicit small arms and light weapons, which make full use of the INTERPOL Illicit Arms Records and Tracing Management System?

(d) Is the State taking steps at the national level to enable the identification and targeting of individuals or groups implicated in the illegal trafficking in weapons, including deactivated firearms?

(e) Does the State have in place national measures for the detection, collection, seizure and disposal of illegal arms and explosives?

(f) Has the State established a network of national points of contact on improvised explosive devices?

(g) Is the State taking measures at the national level to prevent the smuggling and illicit diversion of precursor chemicals that could be used to build improvised explosive devices?

(h) Does the State conduct frequent risk and threat assessments of illegal trafficking in the State through law enforcement work (in terms of the risks, pervasiveness, types of arms, statistics and impact on law and order)?

(i) Has the State established national law-enforcement coordinating mechanisms among concerned agencies to counter arms trafficking?

(j) Does the State join regional and international law-enforcement cooperation mechanisms to prevent and combat arms trafficking (e.g., police working groups or regional police agencies)?

(k) Does the State utilize the INTERPOL I-24/7 network and the World Customs Organization Customs Enforcement Network Communication Platform (CENcomm) network, wherever possible, in order to enhance coordination and information-sharing both among Member States and between Governments and the private sector, to prevent the flow of components of improvised explosive devices, such as chemical components, detonators and detonating cords?

4. Member States should have in place a customs border-control programme to detect and prevent the smuggling of small arms and light weapons and explosives.

156. The following issues should be considered:

(a) Has the State implemented a risk management programme?

(b) Has the State established links with licensing authorities to verify the validity of issued licences?

(c) Is the State able to receive advance electronic information from importers and exporters?

(d) Has the State put in place an inspection programme? Does this programme include the verification of markings?

(e) Does the State have the resources and capacity to establish special mechanisms or facilities, where needed, to screen women and girls? Has the State introduced a programme to recruit more women in the security sector to enhance border security mechanisms?

(f) Has the State put in place comprehensive import/export/transit movement controls administered by customs for arms, ammunition and explosives?

(g) Has the State established cross-border cooperation between customs administrations? (See also chapter II, section O, “Effective border security and related issues”, subsection 11, “Coordination with regional and international partners”.)

(h) Has the State established trade partnership programmes?

(i) Does the State prevent the use of Internet and information technology tools to print three-dimensional illicit firearms, their parts and components, and ammunition?

157. The following international instruments, standards and good practices provide guidance in this area:

(a) Addendum to the Madrid Guiding Principles, guiding principle 52;

(b) Mine Action Service, “Improvised explosive device lexicon”, 2019, available at www.unmas.org/en/publications;

(c) INTERPOL Project Watchmaker, which enables INTERPOL member countries to identify and track known or suspected individuals involved in the

manufacture or use of explosives. This is achieved through working groups that facilitate the exchange of biometric data and document records;

(d) World Customs Organization/INTERPOL/UNODC Programme Global Shield to secure global supply chains and enhance public safety aiming at preventing smuggling and the illicit diversion of precursor chemicals that could be used to build improvised explosive devices.

158. For issues relating to employee integrity programmes, see also chapter II, section O, "Effective border security and related issues", subsection 2, "Strategy and awareness".

D. Taking the steps necessary to prevent the commission of terrorist acts, through the provision of early warning

1. Preventing the commission of terrorist acts

159. Member States should have in place a national comprehensive and integrated counter-terrorism strategy, policy or government-wide programme to prevent the commission of terrorist acts. The national counter-terrorism strategy should state how the Government intends to counter terrorism and should ideally also incorporate both "prevention" and "response" elements. The strategy should also define an institutional structure comprised of all agencies with a counter-terrorism mandate, establish clear roles for each and provide for their coordination. The strategy should also include measures to engage other levels of government, civil society and other States and inform them of how the Government seeks to prevent terrorism.

160. In many Member States, police and other law enforcement agencies play a critical role in the prevention of terrorist acts. A number of strategies, policies and good practices employed by Member States could be used by national law enforcement organizations to prevent the commission of terrorist acts. A robust, intelligence-led law enforcement capacity assists in the identification and disruption of terrorist threats. The effectiveness of the law enforcement response also relies on prevention, which is most effective when law enforcement works closely with local communities through measures such as community policing.

161. In its resolution 2341 (2017), the Council calls upon Member States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, which should include, inter alia, assessing and raising awareness of the relevant risks, taking preparedness measures, including effective responses to such attacks, promoting better interoperability in security and consequence management and facilitating effective interaction of all stakeholders involved. In the resolution, the Council further calls upon Member States to cooperate actively in the prevention, protection, mitigation, preparedness, investigation, response to, or recovery from, terrorist attacks planned or committed against critical infrastructure.

162. In its resolution 2396 (2017), the Council stresses the need for Member 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 upon Member States to establish or strengthen national, regional and international partnerships with public and private stakeholders to share information and experience in order to prevent, protect, mitigate, investigate, respond to, and recover from, damage from terrorist attacks against "soft" targets.

163. In paragraph 9 (a) of resolution 2322 (2016), the Council calls upon all States to exchange information in accordance with international and domestic law and to

cooperate on administrative, police and judicial matters in order to prevent the commission of terrorist acts and counter the threat of foreign terrorist fighters, including returnees. In paragraph 18, the Council encourages Member States and international, regional and subregional organizations to consider the possibility of developing round-the-clock counter-terrorism networks, taking into account their existing cooperation arrangements.

164. Member States should put in place operational measures for the adoption of an appropriate structure to prevent the commission of terrorist acts, which should include:

(a) A central high-level committee or agency for the development and coordination of a national counter-terrorism policy;

(b) A central body (national counter-terrorism centre) to integrate, analyse and evaluate all operational and strategic information provided by all national law enforcement agencies with a counter-terrorism mandate. The centre should bring together representatives of all relevant national law enforcement agencies with a counter-terrorism mandate to fuse intelligence and flag instances in which information from one agency would be useful to other agencies;

(c) A forensic science capacity, which should have access to equipment and facilities to process physical evidence;

(d) A dedicated, highly specialized counter-terrorism unit within the police or relevant law enforcement agency, supported by clear command and control mechanisms;

(e) A national intelligence capacity that can clearly understand and depict the national and international terrorism situation, conduct terrorism threat assessments and, where applicable, transfer relevant intelligence related to terrorism threats that may be of use in identifying terrorists, including foreign terrorist fighters, to the competent law enforcement authorities of the same State or to authorities of a foreign State, in accordance with national law and international human rights law;

(f) Policies, mechanisms and procedures to ensure the effective exchange of information, including information obtained from intelligence agencies, concerning the identity and activities of terrorists, including foreign terrorist fighters, among all relevant national law enforcement agencies;

(g) Measures to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to, and recover from, damage from terrorist attacks on critical infrastructure facilities, “soft” targets, vulnerable targets and tourism sites, including through joint training and the use or establishment of relevant communication or emergency warning networks;

(h) A central counter-terrorism database accessible, on a need-to-know basis, to all relevant law enforcement agencies, with oversight mechanisms and appropriate limitations on use of the information, in accordance with human rights principles;

(i) Access to international counter-terrorism databases for all relevant law enforcement and security agencies;

(j) An alert/arrest message capacity at the national level, including with border police, which is operational on a 24 hours a day, seven days a week basis;

(k) Legislative mandates and oversight of the activities of law enforcement and intelligence agencies in order to prevent the misuse of authority or abuse of discretion;

(l) A public telephone line (“hotline”) or website to report suspicious behaviour or activity.

165. Member States should also have in place an enforcement programme for preventing the commission of terrorist acts. The following issues should be considered in that regard:

(a) Does the State have in place a comprehensive and integrated counter-terrorism strategy that engages a wide range of stakeholders (e.g., academia, the media, civil society) beyond law enforcement agencies?[79]

(b) Does the State have in place a mechanism for implementing such a strategy?[80]

(c) Does the State have in place a national law enforcement strategy to counter terrorism?[81]

(d) Does the State have in place a law enforcement structure for the implementation of the national law enforcement strategy to counter terrorism?[82]

(e) Is the law enforcement structure supported by technology and equipment (including databases, biometrics and communications)?[83]

(f) Are criminal investigators able to collect evidence using special investigative techniques?[84]

(g) Do the State’s law enforcement agencies conduct threat and risk assessments relating to terrorism,[85] including on the prevention, protection, mitigation, preparedness, investigation, response to, or recovery from, terrorist attacks planned or committed against critical infrastructure, soft targets, vulnerable targets and tourism sites? Is the State’s relevant law enforcement agency capable of monitoring, collecting and analysing data from social media platforms in order to advance investigations or to prevent the flow of foreign terrorist fighters in a manner that is compliant with States’ international human rights obligations?[86]

(h) Does the State have in place a round-the-clock alert/arrest message capacity at the national level, including with border police?[87]

(i) Is there an existing regional and/or subregional arrangement for police cooperation or round-the-clock network to counter terrorism. If so, is the State taking part in it or considering doing so?[88]

166. For issues relating to community policing, see also chapter II, section A, “Suppressing and preventing recruitment”; for issues relating to the exchange of information among law enforcement agencies, see also chapter III, section A, “Exchanging information”; for issues relating to inter-agency coordination, see also chapter II, section O, “Effective border security and related issues”, subsection 11, “Coordination with regional and international partners”.

[79] Resolution 2395 (2017), para. 16.
[80] Ibid.
[81] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.3.2.
[82] Ibid., template 2.3.3.
[83] Ibid., template 2.3.4.
[84] Madrid Guiding Principles, guiding principle 25.
[85] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.3.7.
[86] Madrid Guiding Principles, guiding principles 25 and 26.
[87] Madrid Guiding Principles, guiding principle 17.
[88] Resolution 2322 (2016), para. 18.

167. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principles 11, 15–19 and 25–27;

(b) Addendum to the Madrid Guiding Principles, guiding principle 50;

(c) Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight (A/HRC/14/46);

(d) Code of Conduct for Law Enforcement Officials (General Assembly resolution 34/169, annex);

(e) Organization for Security and Cooperation in Europe (OSCE), *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach* (Vienna, February 2014);

(f) European Commission, Radicalization Awareness Network, *Collection of Approaches and Practices: Preventing Radicalisation to Terrorism and Violent Extremism* (2019), in particular the sections on infrastructure for countering violent extremism;

(g) Global Counterterrorism Forum, The Hague-Marrakech Memorandum on Good Practices for a More Effective Response to the Foreign Terrorist Fighter Phenomenon, good practice 10.

2. Early warning

168. Member States should actively communicate information about potential terrorist threats to counterparts in other Member States. States should also share relevant information to prevent cross-border movement of terrorists, including foreign terrorist fighters, such as details of their identity, travel documents or means of travel, upon which border authorities and other relevant agencies can make timely and informed decisions for further action.[89] In order to ensure a centralized approach and to avoid duplication of efforts, Member States should designate a law enforcement office to serve as the focal point for requests related to countering terrorism. States should also develop the capacity to monitor threats and evaluate information (“analysis function”) and strive to communicate information that would be useful to other States.

169. Member States should make full use of existing mechanisms to alert other States. The INTERPOL I-24/7 secure global police communications system is available through the INTERPOL National Central Bureaus to access, receive, share, check and disseminate police information in real time throughout the world. Member States should seek to extend the I-24/7 system beyond the National Central Bureaus to counter-terrorism units and other law enforcement agencies, enabling all relevant authorities to access international databases, including nominal data on criminals, stolen and lost travel documents, fingerprints, DNA and stolen motor vehicles, maintained by INTERPOL.[90] States should seek to transmit, through INTERPOL communication tools, critical crime-related information, including information on wanted individuals, known or suspected foreign terrorist fighters, possible threats, dangerous materials and criminals’ modus operandi using the organization’s system

[89] Resolutions 2178 (2014) and 2322 (2016), and Madrid Guiding Principles, guiding principle 17.
[90] Resolution 2322 (2016), para. 17.

of international color-coded notices, as well as the INTERPOL-United Nations Security Council Special Notice.[91]

170. Member States should share information related to cargo security and other customs matters through the Customs Enforcement Network secure platform and the Regional Intelligence Liaison Office network of the World Customs Organization.

171. The following issues should be considered:

(a) Does the State utilize early-warning systems regarding terrorism and other related criminal activities?[92]

(b) Does the State have access to national, regional and international sources of information on foreign terrorist fighters?[93]

(c) Does the police or the relevant law enforcement agency seek to communicate information about potential terrorist threats, terrorists (including foreign terrorist fighters) or terrorist activities to counterparts in other Member States?[94]

(d) Do the national law enforcement and security agencies actively transmit relevant information that may be of use in identifying existing or potential foreign terrorist fighters?[95]

(e) Does the State seek to expand access to, and ensure the effective utilization of, the global information-sharing tools of INTERPOL among national law enforcement, immigration and border agencies?[96]

172. For issues relating to the capacity of law enforcement agencies, see also chapter III, section A, “Exchanging information”; for issues relating to the use of the Customs Enforcement Network secure platform and the Regional Intelligence Liaison Office network of the World Customs Organization, see also chapter III, section A, “Exchanging information”.

173. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principles 15–19;

(b) Addendum to the Madrid Guiding Principles, guiding principle 50;

(c) African Union, *African Union Continental Early Warning System: The CEWS Handbook* (Addis Ababa, 21 February 2008);

(d) Global Counterterrorism Forum, The Hague-Marrakech Memorandum on Good Practices for a More Effective Response to the Foreign Terrorist Fighter Phenomenon, good practice 10.

E. Denying safe haven

174. In paragraph 2 (c) of resolution 1373 (2001), the Council requires all States to deny safe haven to those who finance, plan, support or commit terrorist acts. In this

[91] To alert law enforcement agencies to individuals and entities that are subject to United Nations sanctions because of their affiliation with Al-Qaida or the Taliban.

[92] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.3.10.

[93] Madrid Guiding Principles, guiding principle 15.

[94] Ibid.

[95] Ibid.

[96] Madrid Guiding Principles, guiding principle 17.

regard, there are several measures that need to be considered collectively with due respect for human rights. These include legislative measures criminalizing the provision of safe haven and measures providing adequate jurisdiction for the prosecution of such offences. Practical and legal measures on immigration, border control and exchange of information[97] should be in place to ensure that States have the capacity to deny safe haven and bring to justice those who harbour terrorists and those who finance, plan, facilitate or incite terrorist acts.[98]

175. The United Nations counter-terrorism instruments provide that any person who is taken into custody for purposes of extradition on charges of terrorist offences shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in conformity with the law of the State in the territory of which that person is present and applicable provisions of international law, including international human rights law.[99]

176. The following issues should be considered:

(a) Has the State criminalized the harbouring of terrorists?[100]

(b) Does the law contain a clear definition of "harbouring" (e.g., "intentionally concealing, hindering or preventing the apprehension of a person who has committed or is planning to commit a terrorist act or is a member of a terrorist group")?

(c) Does the State have in place legislation to penalize persons or organizations involved in intentionally concealing, hindering or preventing the apprehension of any person in the knowledge that such person has committed or is planning to commit a terrorist act or is a member of a terrorist group?[101]

(d) Does the State have in place adequate legal measures on jurisdiction? (See also chapter II, section J, "Investigating, prosecuting and adjudicating terrorist acts".)

(e) Does the State have in place legal measures facilitating the gathering of information and mechanisms for domestic and international exchange of information? (See also chapter III, section A, "Exchanging information".)

F. Preventing the use of territory for the purpose of terrorist acts

177. In paragraph 2 (d) of resolution 1373 (2001), the Council requires all States to take measures to prevent those who finance, plan, facilitate or commit terrorist acts from using their territories for those purposes against other States or their citizens.

178. Furthermore, in paragraph 6 (c) of resolution 2178 (2014), the Council requires all States to ensure that their domestic laws and regulations establish as serious criminal offences sufficient to provide the ability to prosecute and to penalize the wilful organization, or other facilitation, by their nationals or in their territories, of the travel of individuals to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. In this regard, in order to prevent the use of territory for the purpose of terrorist acts, Member States should

[97] Resolution 1373 (2001), para. 2 (b).
[98] Ibid., para. 2 (c); and resolution 1624 (2005), para. 1 (c).
[99] See art. 17 of the Convention for the Suppression of the Financing of Terrorism, art. 14 of the International Convention for the Suppression of Terrorist Bombings, and art. 12 of the International Convention for the Suppression of Acts of Nuclear Terrorism.
[100] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.4.1.
[101] Ibid., template 2.4.2.

take into consideration cooperation on border-security measures with neighbouring States.

179. The following issues should be considered:

(a) Is it possible to prosecute any preparatory or accessory acts that are conducted in the State with the aim of committing terrorist acts against other States or their citizens outside the State's territory?[102] (See also chapter II, section J, "Investigating, prosecuting and adjudicating terrorist acts".)

(b) Is the State able to combat the use of fraudulent travel documents in order to strengthen the security of its international borders? (See also chapter II, section O, "Effective border security and related issues", subsection 3, "Documentation".)

180. The following international instruments, standards and good practices provide guidance in this area:

(a) United Nations Convention against Transnational Organized Crime, 2000;

(b) International Organization for Migration (IOM), *Passport Examination Procedure Manual*, 2nd ed. (Geneva, June 2016);

(c) World Customs Organization/International Air Transport Association/ICAO, "Guidelines on advance passenger information", 2014;

(d) ICAO, *Guidelines on Passenger Name Record (PNR) Data* (Doc. 9944) (Montreal, 2010);

(e) Office of the United Nations High Commissioner for Refugees (UNHCR), "Addressing security concerns without undermining refugee protection", Rev.2, 17 December 2015;

(f) OSCE, Decision No. 6/06 on the further measures to prevent the criminal use of lost/stolen passports and other travel documents, 6 December 2006.

181. See also chapter II, section O, "Effective border security and related issues".

G. Codification

182. In paragraph 3 (d) of resolution 1373 (2001), the Council calls upon all States to become parties as soon as possible to the relevant international conventions and protocols relating to terrorism. Member States should criminalize the offences that are outlined in the relevant international counter-terrorism legal instruments to which they are a party or as required by the relevant Council resolutions.

183. In paragraph 4 of resolution 2322 (2016), the Council recognizes the important role of national legislation in enabling international judicial and law enforcement cooperation on terrorist-related offences and calls upon Member States to enact and, where appropriate, review their respective counter-terrorism laws in view of the evolving threat posed by terrorist groups and individuals. In paragraph 11, the Council also urges, as a matter of priority, that Member States consider, as appropriate, ratifying, acceding to and implementing other relevant international conventions to support international cooperation in criminal matters, such as the United Nations Convention against Transnational Organized Crime of 2000 and the Protocols thereto.

184. Member States' legislation should also criminalize the attempt to commit the offences, acting as an accomplice and/or being a party to the offence, through an

[102] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.5.1.

offence of conspiracy or otherwise, and impose penalties that reflect the serious nature of the offences.

185. Additional elements that Member States should also take into consideration include the precision with which the terrorist acts are defined (whether these are overly broad or vague) and whether they have the potential for human rights abuse. Shortcomings in these areas may detract from the actual implementation and/or effectiveness of the overall measures.

186. Depending on their respective legal traditions, Member States may approach codification differently (e.g., through the use of specific counter-terrorism legislation, amendments to the criminal code or amendments across different pieces of legislation).

187. UNODC has developed model laws as technical assistance tools to assist Governments to incorporate their obligations under international treaties into national legislative provisions. The model provisions are meant to assist with, but not to substitute for, the meticulous process of drafting a law. To the extent permitted by the relevant international conventions, individual States will need to make adjustments to the text to more accurately reflect the fundamental principles of their legal systems and constitutions.

188. With regard to the international counter-terrorism instruments, resolution 1373 (2001) contains two distinct requirements. The present section addresses the establishment of terrorist acts as serious criminal offences in domestic laws, as required in paragraph 2 (e) of the resolution. Thus, the section deals only with the criminal requirements of the international instruments.

189. Since some elements of these instruments are non-criminal in nature, it is not sufficient simply to assess criminalization. Therefore, in paragraph 3 of the resolution, the Council calls upon all States to become a party to and implement the international instruments. (Non-criminal requirements of the international counter-terrorism instruments are addressed in chapter III, section C, “Ratifying the international counter-terrorism instruments”.)

190. Pursuant to resolution 2178 (2014), Member States are required to prevent and suppress the recruiting, organizing, transporting or equipping of individuals who travel to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, and the financing of travel and of their activities.

191. In paragraph 1 of resolution 2396 (2017), the Council recalls its decision, contained in resolution 2178 (2014), that all Member States should establish serious criminal offences regarding the travel, recruitment and financing of foreign terrorist fighters and urges Member States to fully implement their obligations in that regard, including to ensure that their domestic laws and regulations establish serious criminal offences sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offence.

192. The following issues should be considered:

(a) Does the State’s domestic law criminalize all the offences set forth in the international counter-terrorism instruments?

(b) Does the State’s domestic law criminalize all the offences set forth in the international counter-terrorism instruments to which it is a party?

(c) If the State defines terrorist acts in its legislation, is the definition sufficiently clear and precise so as not to apply to acts beyond those envisaged by the

international counter-terrorism instruments (i.e., acts said to threaten national security or stability without further elaboration, conventional crimes, or non-violent acts of protest or dissent)?

(d) Does the State criminalize acts of directing and/or organizing terrorist acts?[103]

(e) Does the State criminalize knowingly assisting an offender to evade investigation, prosecution or punishment?[104]

(f) Does the State criminalize attempts to commit a terrorist act?

(g) Does the State criminalize making a threat to commit an offence when the circumstances indicate that the threat is credible?[105] (See also chapter II, section I, "Criminalizing acts associated with foreign terrorist fighters".)

193. With respect to the 19 international counter-terrorism instruments, Member States should note, in particular, the following:

(a) **Convention on Offences and Certain Other Acts Committed on Board Aircraft, 1963**. The Convention does not contain criminal requirements. Its implementation is addressed in chapter III, section C, "Ratifying the international counter-terrorism instruments";

(b) **Convention for the Suppression of Unlawful Seizure of Aircraft, 1970**. The Convention requires States parties to criminalize seizing, or exercising control of, an aircraft, unlawfully, by force, threat thereof or intimidation, by a person on board an aircraft;

(c) **Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 1971**. The Convention requires States parties to:

(i) Make it an offence for any person on board an aircraft in flight to unlawfully, by force or threat thereof, or any other form of intimidation, seize or exercise control of that aircraft or to attempt to do so;

(ii) Make hijackings punishable by severe penalties;

(iii) Take custody of offenders and to either extradite the offender or submit the case for prosecution and assist one another in connection with criminal proceedings brought under the Convention;

(d) **Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 1988**. The Protocol requires States parties to criminalize:

(i) Unlawfully and intentionally performing an act of violence against a person at an airport serving international civil aviation that causes, or is likely to cause, serious injury or death;

(ii) Unlawfully and intentionally destroying or seriously damaging the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupting the services of the airport, if such an act endangers, or is likely to endanger, safety at that airport;

[103] Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation.
[104] Ibid.
[105] Ibid.

(e) **Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, 2010**. The Convention requires States parties to criminalize:

(i) Using civil aircraft for the purposes of causing death, serious bodily injury or serious damage;

(ii) Using civil aircraft to release or discharge any biological, chemical or nuclear weapon or similar substance to cause death, serious bodily injury or serious damage;

(iii) Using any biological, chemical or nuclear weapon or similar substance on board or against civil aircraft;

(iv) Using civil aircraft to unlawfully transport any biological, chemical or nuclear weapon, related material or other dangerous material;

(v) Committing cyberattacks on air navigation facilities;

(vi) Directing and organizing such offences;

(f) **Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, 2010**. The Protocol requires States parties to:

(i) Make it an offence to hijack an aircraft through technological means;

(ii) Direct and/or organize such an offence;

(g) **Protocol to amend the Convention on Offences and Certain Other Acts Committed on Board Aircraft, 2014**. The Protocol expands jurisdiction over offences and acts committed on board aircraft from the State of registration of the aircraft to the State of the operator and the State of landing;

(h) **Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, 1973**. The Convention requires States parties to criminalize:

(i) Intentionally murdering, kidnapping or committing another attack upon the person or liberty of an internationally protected person;

(ii) Committing a violent attack upon the official premises, private accommodations or means of transport of such a person;

(iii) Threatening or attempting to commit or acting as an accomplice in such an attack;

(i) **International Convention against the Taking of Hostages, 1979**. The Convention requires States parties to make it an offence to seize or detain and threaten to kill, to injure or to continue to detain another person in order to compel a third party, namely, a State, an international intergovernmental organization, a natural or juridical person or a group of persons, to do, or abstain from doing, any act as an explicit or implicit condition for the release of the hostage;

(j) **Convention on the Physical Protection of Nuclear Material, 1980**. The Convention requires States parties to criminalize:

(i) Unlawfully receiving, possessing, using, transferring, altering, disposing, dispersing, robbing, embezzling or fraudulently obtaining nuclear material;

(ii) Demanding nuclear material by threat or use of force or by any other form of intimidation;

(iii) Threatening to use nuclear material to cause death, serious injury or substantial property damage and threatening to commit the theft or robbery of

nuclear material in order to compel a natural or legal person, international organization or State to do or to refrain from doing any acts;

(k) **Amendment to the Convention on the Physical Protection of Nuclear Material, 2005**. The Amendment does not contain criminal requirements. Its implementation is addressed in chapter III, section C, "Ratifying the international counter-terrorism instruments";

(l) **International Convention for the Suppression of Acts of Nuclear Terrorism, 2005**. The Convention requires States parties to criminalize:

(i) Unlawfully possessing radioactive material or making or possessing a device with the intent to cause death or serious bodily injury, or to cause substantial damage to property or to the environment;

(ii) Using radioactive material or devices to damage a nuclear facility in a manner that releases or risks the release of radioactive material, with the intent to cause death, serious bodily injury, substantial damage to property or the environment, or to compel a natural or legal person, an international organization or a State to do or refrain from doing an act;

(iii) Threatening, under circumstances that indicate the credibility of the threat, to commit the act described in subparagraph (ii) above;

(iv) Unlawfully demanding radioactive material, devices or facilities by threat or force;

(m) **Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988**. The Convention requires States parties to criminalize:

(i) Unlawfully and intentionally seizing or exercising control over a ship by force, threat thereof or intimidation;

(ii) Performing an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of the ship;

(iii) Placing a destructive device or substance aboard a ship;

(iv) Committing other acts against the safety of ships;

(n) **Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation**. The Protocol requires States parties to criminalize:

(i) Using a ship as a device to further an act of terrorism;

(ii) Knowingly transporting on board a ship various materials intended to be used to cause, or in a threat to cause, death or serious injury or damage to further an act of terrorism, or persons who have committed an act of terrorism;

(o) **Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, 1988**.

(i) The Protocol provides that articles 5 and 7 and 10 to 16 of the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, including the exercise of jurisdiction, the *aut dedere aut judicare* rule and extradition, shall apply mutatis mutandis to the offences defined in the Protocol where such offences are committed on board or against fixed platforms located on the continental shelf;[106]

[106] Although the definition of "fixed platform" refers to the seabed only, the preamble, articles 1 (1), 3 and 4, and indeed the title of the Protocol, all refer to the "continental shelf". Article 76 of the United Nations Convention on the Law of the Sea of 1982 defines the continental shelf of a coastal State as comprising the seabed and subsoil of the submarine areas that extend beyond its

(ii) The Protocol requires State parties to criminalize, unlawfully and intentionally:

a. Seizing or exercising control over a fixed platform by force or threat thereof or any other form of intimidation;

b. Performing an act of violence against a person on board a fixed platform if that act is likely to endanger its safety;

c. Destroying a fixed platform or causing damage to it that is likely to endanger its safety;

d. Placing or causing to be placed on a fixed platform, by any means whatsoever, a device or substance that is likely to destroy that fixed platform or likely to endanger its safety;

e. Injuring or killing any person in connection with the commission or the attempted commission of any of the above-mentioned offences;

f. Attempting, abetting, or acting as an accomplice in, any of the above-mentioned offences;

g. Threatening, with or without a condition, as provided for under national law, aimed at compelling a physical or juridical person to do or refrain from doing any act, to commit a number of the offences mentioned above, provided that the threat is likely to endanger the safety of the fixed platform;

(p) **Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf**. The Protocol adapts the changes to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation to the context of fixed platforms located on the continental shelf;

(q) **Convention on the Marking of Plastic Explosives for the Purpose of Detection, 1991**. The Convention does not contain criminal requirements. Its implementation is addressed in chapter III, section C, “Ratifying the international counter-terrorism instruments”;

(r) **International Convention for the Suppression of Terrorist Bombings, 1997**. The Convention requires States parties to establish jurisdiction over and criminalize the unlawful and intentional use of explosives and other lethal devices in, into or against various defined public places with the intent to cause death or serious bodily injury, or with the intent to cause extensive destruction of a public place. Parties are also required to criminalize attempting, or participating as an accomplice in, such an offence;

(s) **International Convention for the Suppression of the Financing of Terrorism, 1999**. The Convention requires States parties to:

(i) Criminalize the direct or indirect, unlawful and wilful, provision or collection of funds with the intention that they be used, or in the knowledge that they are to be used, in full or in part, in order to carry out any act that constitutes an offence within the scope and as defined in the treaties annexed to the

territorial sea throughout the natural prolongation of its land territory to the outer edge of the continental margin, or to a distance of 200 nautical miles from the baselines from which the breadth of the territorial sea is measured where the outer edge of the continental margin does not extend up to that distance. The “continental margin” is defined in the same article as comprising the submerged prolongation of the land mass of the coastal State, and consisting of the seabed and subsoil of the shelf, the slope and the rise. It does not include the deep ocean floor. These terms are further explained in R. Churchill and A. Lowe, *The Law of the Sea*, 3rd ed. (Manchester, Manchester University Press, 1999), on pp. 141 to 159, and with an illustration on p. 30.

Convention[107] or any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act, and to cooperate in the prevention of those acts;

(ii) Afford one another the greatest measure of assistance in connection with criminal investigations or criminal or extradition proceedings in respect of the offences set forth in the Convention, including assistance in obtaining evidence in their possession necessary for the proceedings.

194. For further requirements, see also chapter I.

H. Preventive offences and preparatory acts

195. A core requirement of resolution 1373 (2001), set forth in paragraph 2 (e), is that all States shall ensure that their domestic laws and regulations establish terrorist acts as serious criminal offences and that the punishment duly reflects the seriousness of the offence. Furthermore, pursuant to the same paragraph, States must ensure that their domestic legal systems establish as offences acts involving the participation in the financing, planning, preparation, perpetration or support of terrorist acts. In resolution 2178 (2014), the Council reaffirms States' obligations under resolution 1373 (2001) and, in paragraph 5, decides that Member States shall, consistent with international human rights law, international refugee law and international humanitarian law, prevent and suppress the recruiting, organizing, transporting or equipping of individuals who travel to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, and the financing of their travel and of their activities. In addition, in paragraph 6, the Council requires all States to ensure that their domestic laws and regulations establish as serious criminal offences sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offence the travel or attempted travel for any of the above-mentioned purposes, the wilful provision or collection, by any means, directly or indirectly, of funds with the intention or in the knowledge that they are to be used to finance travel for any of those purposes, and the wilful organization, or other facilitation, including acts of recruitment, by their nationals or in their territories, of travel for any of those purposes.

196. In its resolution 2341 (2017), the Council calls upon all Member States to ensure that they have established criminal responsibility for terrorist attacks intended to destroy or disable critical infrastructure, as well as the planning of, training for, and financing of, and logistical support for, such attacks.

197. The criminalization of preparatory acts and preventive offences is a critical component of an effective prevention-based counter-terrorism strategy and will assist

[107] Convention for the Suppression of Unlawful Seizure of Aircraft; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents; International Convention against the Taking of Hostages; Convention on the Physical Protection of Nuclear Material; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation; Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf; International Convention for the Suppression of Terrorist Bombings.

the State to effectively bring terrorists to justice.[108] Preparatory or preventive offences do not require, as an element of the offence, that a terrorist attack be attempted or successfully executed. Even though States may differ as to how exactly these offences are defined, establishing clear offences for preparatory acts committed either by the individual or by any other person, association or group will greatly facilitate early intervention by the criminal justice system and increase the potential to reduce violence and thwart attacks.[109] In the criminalization of these acts, Member States should ensure that offences are defined clearly and precisely, in compliance with the principle of legality.[110]

198. In paragraph 7 of resolution 2331 (2016), the Council recalls its decision that all Member States shall 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, and urges all States to ensure that their domestic laws and regulations establish serious criminal offences sufficient to provide the ability to prosecute and penalize in a manner duly reflecting the seriousness of the offence of trafficking in persons committed with the purpose of supporting terrorist organizations or individual terrorists, including through recruitment for the commission of terrorist acts.

199. The following issues should be considered:

(a) Does the State criminalize acts of planning as an autonomous offence?

(b) Does the State criminalize acts of preparation as an autonomous offence?

(c) Does the State criminalize acts of support as an autonomous offence?

(d) Does the State criminalize acts of providing training as an autonomous offence?

(e) Does the State criminalize acts of receiving training as an autonomous offence?

(f) Does the State criminalize foreign terrorist fighter-related offences? (See also the following section on criminalizing foreign terrorist fighter offences.)[111]

(g) Does the State criminalize terrorist attacks intended to destroy or disable critical infrastructure and other related offences?[112]

(h) Has the State criminalized the offence of trafficking in persons committed with the purpose of supporting terrorist organizations, or individual terrorists, including through the financing of and recruitment for the commission of terrorist acts?[113]

[108] See S/2015/123, annex.

[109] Ibid.

[110] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (A/HRC/31/65).

[111] Resolution 2178 (2014).

[112] Resolution 2341 (2017).

[113] Resolution 2331 (2016), para. 7. See also resolution 2322 (2016), para. 11, in which the Council urges as a matter of priority that Member States consider, as appropriate, ratifying, acceding to and implementing relevant international conventions to support international cooperation in criminal matters, such as the United Nations Convention against Transnational Organized Crime and the Protocols thereto, including the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime.

(i) Does the State criminalize all forms and aspects of trafficking in cultural property and related offences that benefit or may benefit terrorists or terrorist groups?[114]

(j) Does the State's legislation comply with the principle of legality enshrined in article 15 of the International Covenant on Civil and Political Rights, such that criminal liability is narrowly and clearly defined?[115]

200. The following international instruments provide guidance in this area: Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol.

I. Criminalizing acts associated with foreign terrorist fighters

201. Pursuant to resolution 2178 (2014), Member States are required to prevent and suppress the recruiting, organizing, transporting or equipping of individuals who travel to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, and the financing of their travel and of their activities. Reiterating the requirement that terrorists are to be brought to justice, the Council, in the same resolution, decides that all States shall ensure that their domestic laws and regulations establish as serious criminal offences sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offence:

(a) The travel or attempted travel by their nationals to a State other than their States of residence or nationality, and the travel or attempted travel by other individuals from their territories to a State other than their States of residence or nationality, for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training;

(b) The wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds be used, or in the knowledge that they are to be used, in order to finance the travel of individuals who travel to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training;

(c) The wilful organization, or other facilitation, including acts of recruitment, by their nationals or in their territories, of the travel of individuals who travel to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

202. In paragraph 1 of resolution 2396 (2017), the Council recalls its decision, contained in its resolution 2178 (2014), that all Member States shall establish serious criminal offences regarding the travel, recruitment and financing of foreign terrorist fighters, and urges Member States to fully implement their obligations in that regard, including to ensure that their domestic laws and regulations establish serious criminal offences sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offence.

203. In order to ensure that they have in place the appropriate legal tools to address the evolving foreign terrorist fighter phenomenon, States may need to amend their existing laws or introduce new laws to meet the requirements of resolutions 1373 (2001), 1624 (2005), 2178 (2014) and 2396 (2017). Member States are required by

[114] Resolution 2322 (2016), para. 12.
[115] A/HRC/31/65.

those resolutions to establish preparatory and inchoate offences, including the planning and preparing to travel as a foreign terrorist fighter; the organizing, facilitating and financing of the travel of foreign terrorist fighters; and the receiving of terrorist training, in compliance with international human rights law.

204. Member States should also put in place special safeguards and legal protections to ensure that appropriate action is taken in cases involving children, in full compliance with their obligations under international law.[116] (For more information concerning children and children's rights in the context of counter-terrorism, see also chapter IV, section H, "Complying with international human rights, refugee and humanitarian law".)

205. The following issues should be considered:

(a) Does national legislation criminalize the full range of conduct relating to foreign terrorist fighters, including preparatory and inchoate acts, and as required by resolutions 1373 (2001), 1624 (2005), 2178 (2014) and 2396 (2017)?

(b) Does the State criminalize travel by nationals for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts?

(c) Does the State criminalize travel by nationals for the purposes of providing or receiving terrorist training?

(d) Does the State criminalize travel by nationals for the purpose of the facilitation, including organizing, transporting and equipping, of the travel of foreign terrorist fighters?

(e) Does the State criminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds be used, or in the knowledge that they are to be used, in order to finance the travel of individuals who travel to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training? (For issues relating to the criminalization of the financing of terrorism, see also chapter I, section A, "Criminalizing the financing of terrorism".)

(f) Does the State criminalize the wilful organization, or other facilitation, including acts of recruitment, by its nationals or in its territories, of the travel of individuals who travel to a State other than their States of residence or nationality for the purposes of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training?

(g) How does the State address the movement of minors (e.g., parents taking children to territory controlled by ISIL (Da'esh)), especially young girls who may be vulnerable to sexual violence, forced marriage and denial of education, upon arrival?

(h) Are the above-mentioned criminal offences clearly defined?

(i) Are penalties for terrorism-related crimes, including those of foreign terrorist fighters, commensurate with their gravity?

(j) Is the State's domestic legislation in accordance with its obligations under international law?

206. The following international instrument provides guidance in this area: Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, 2015.

[116] Addendum to the Madrid Guiding Principles, guiding principle 42.

J. Investigating, prosecuting and adjudicating terrorist acts

207. The prosecution of terrorism cases, including those related to foreign terrorist fighters, continues to be at times significantly challenged by the difficulty of collecting sufficient admissible evidence to secure a conviction. Generating admissible evidence and converting intelligence into admissible evidence against foreign terrorist fighters are complex and multifaceted tasks. The processing of foreign terrorist fighters in the criminal justice system, in some instances, may complicate some aspects of established criminal procedures and evidentiary standards relating to the adjudication of suspected terrorists. The Council, in its resolution 2178 (2014), calls for cooperation in evidentiary matters, stating that States shall assist one another in connection with criminal investigations, including assistance in obtaining evidence.

208. States should consider re-evaluating their methods and best practices, as appropriate, in particular those relating to specialized investigative techniques (including those involving electronic evidence). Improving the collection, handling, preservation and sharing of relevant information and evidence obtained from conflict zones, in accordance with domestic law and Member States' obligations under international law, is of paramount importance and an area in which the Working Group on Criminal Justice, Legal Responses and Countering the Financing of Terrorism of the United Nations Global Counter-Terrorism Coordination Compact is developing guidelines.

209. Successfully handling complex terrorism-related cases, in particular cases related to foreign terrorist fighters, increasingly depends on making effective use of evidence collected through special investigative techniques, digital evidence, forensic evidence, information collected by the military and financial intelligence. (For more information on the use of financial intelligence and proceedings, see also chapter I, section F, "Using financial intelligence for investigations and proceedings".)

210. In its resolution 2341 (2017), the Council underlines the need for States to develop the capacity to prevent and disrupt terrorist plots against critical infrastructure where possible, to minimize impacts and recovery time in the event of damage from a terrorist attack, to identify the cause of damage or the source of an attack, to preserve evidence of an attack and to hold those responsible for the attack accountable.

211. In the Madrid Guiding Principles, the Counter-Terrorism Committee provides guidance for investigating and prosecuting criminal offences to stem the flow of foreign terrorist fighters (see guiding principles 25–29). In its addendum to the Madrid Guiding Principles, the Committee provides additional guidance on handling intelligence threat data on foreign terrorist fighters by using special investigative techniques; gathering digital data; and intensifying and accelerating the exchange of relevant operational information and financial intelligence (see guiding principles 43–45).

1. Investigation

(a) Special investigative techniques

212. Special investigative techniques are techniques applied by the competent authorities in the context of criminal investigations for the purposes of detecting and investigating serious crimes and suspects, aimed at gathering information in such a way as to not alert the subjects of the investigation. Special criminal procedures should be distinguished from special investigative techniques, which are broadly

accepted as a law enforcement tool and are obligatory under a number of international conventions relating to serious crimes.

213. In resolution 1373 (2001), the Council does not require States to authorize special criminal procedures to investigate or prosecute terrorism-related cases. Nonetheless, special investigative techniques have been recognized as a possible component of an effective strategy against serious crimes, including acts of terrorism. The use of special investigative techniques could infringe upon fundamental rights and freedoms, partly because of their covert nature. States should therefore develop the mechanisms necessary to ensure effective oversight of their use. In all circumstances, recourse to special investigative techniques should be guided by the principles of legality, necessity, proportionality and non-discrimination, and should be distinguished from exceptional criminal procedures.

214. States are encouraged to conclude bilateral or multilateral agreements or arrangements, as appropriate, for using such techniques in the context of international cooperation. The Council has called upon all States, in conformity with international law, to consider establishing appropriate laws and mechanisms that allow, inter alia, the creation/use, where appropriate, of joint investigation mechanisms and enhanced coordination of cross-border investigations in terrorism cases.[117]

215. The following issues should be considered:

(a) Does the State's legislation allow for the use of special investigative techniques?

(b) Is the legislation sufficiently broad to cover the available special investigative techniques?

(c) Are the circumstances under which special investigative techniques may be used clearly defined in laws, providing for the adequate control of their use by judicial authorities, prosecution systems[118] or other independent bodies through prior authorization, supervision during the investigation, and ex post facto review?

(d) Which is the competent authority responsible for deciding, supervising or using special investigative techniques?

(e) Is there a time limit on the use of special investigative techniques?

(f) What are the provisions or systems in place, through a legislative body or otherwise, to review both draft and existing counter-terrorism legislation, including any amendments to ordinary criminal procedures, in order to ensure that they comply with human rights obligations?[119]

(g) Has the State put in place, where needed, special investigation and prosecution approaches that are gender sensitive and, for cases involving children, take into account their rights?[120]

(h) Does the State ensure effective protection of witnesses in the context of special investigative techniques?[121]

(i) Do the laws and procedures in place take into account the use of new technologies?

[117] Resolution 2322 (2016), para. 15; see also resolution 2482 (2019), para. 15 (b).
[118] Addendum to the Madrid Guiding Principles, guiding principle 48.
[119] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.7.7.
[120] Addendum to the Madrid Guiding Principles, guiding principle 42.
[121] Ibid., guiding principle 43 (d).

(j) Does the law ensure that competent authorities apply less intrusive investigative methods than special investigative techniques, if such methods are adequate for the offence to be detected, prevented or prosecuted? How does the State take into account the need to prevent arbitrary or unlawful interference with privacy?

(k) Are there procedural rules governing the production and admissibility of evidence and safeguarding the rights of the accused to a fair trial?

(l) Do the responsible authorities have the capacity and expertise to handle intelligence threat data on foreign terrorist fighters and other individual terrorists and information collected by investigative agencies and to convert such data and information, where possible, into admissible evidence, where appropriate and subject to the arrangements of the State's legal system?[122]

(m) Does the State have in place domestic mechanisms to allow for international cooperation in special investigative techniques, including, as appropriate, the creation/use of joint investigation mechanisms?

(n) Does the State use existing good practices and standard operating procedures, including those of INTERPOL, for forensic science procedures, in order to ensure the reliability of forensic evidence in court and promote public confidence?

(o) Does the State have in place bilateral and multilateral arrangements for international cooperation in special investigative techniques (especially with neighbouring States)?

216. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principle 25;

(b) Addendum to the Madrid Guiding Principles, guiding principle 43.

(b) Digital evidence

217. The Council, in its resolution 2322 (2016), notes the significant increase in requests for cooperation in gathering digital data and evidence from the Internet and stresses the importance of considering the re-evaluation of methods and best practices, as appropriate, in particular related to investigative techniques and electronic evidence.

218. In its resolution 2396 (2017), the Council calls upon Member States to take measures to improve the collection, handling, preservation and sharing of relevant information and evidence, in accordance with domestic and international law, including information obtained from the Internet, or in conflict zones; encourages enhancing Member States' capacity to cooperate with the private sector (especially with ICT service providers), in accordance with applicable law, in gathering digital data and evidence in cases relating to terrorism and foreign terrorist fighters; and calls upon Member States to improve international, regional and subregional cooperation, if appropriate through multilateral and bilateral agreements, to prevent the undetected travel of foreign terrorist fighters (especially returning and relocating foreign terrorist fighters) from or through their territories.

219. In response to the increased use by terrorists and terrorist groups of ICT for various purposes, in the Madrid Guiding Principles and the addendum to the Madrid Guiding Principles, the Counter-Terrorism Committee recognizes that Member States should build ICT and forensic capacities and expertise within criminal justice and law enforcement agencies and strengthen the capacity of law enforcement agencies to

[122] Ibid., guiding principle 43.

monitor social media content relating to terrorism as digital evidence for investigation and prosecution and in order to prevent the flow of foreign terrorist fighters, while respecting human rights and fundamental freedoms and consistent with their obligations under domestic and applicable international law.

220. Member States should implement provisions on the expedited preservation of digital data and the expedited preservation and partial disclosure of traffic data as stand-alone measures in their procedural legislations and have a specific legal regime for the search and seizure of stored computer data, while respecting human rights and fundamental freedoms and consistent with their obligations under domestic and applicable international law. Freedom of expression, freedom of thought, conscience and religion, and freedom of belief and opinion, as well as the right not to be subjected to arbitrary or unlawful interference with privacy,[123] are human rights relevant to the exchange of data. In this respect, it is important to recall that any infringement upon the right to privacy must comply with the principles of necessity and proportionality as well as non-discrimination. Any international transfer of such information should be essential to the objective of the investigation and described in such a way as to prevent the disclosure of data that is not strictly relevant or necessary.

221. Member States should consider encouraging private companies to establish round-the-clock mechanisms for cooperation with law enforcement and clear rules for the preservation of digital evidence and emergency disclosure requests.

222. States should also consider encouraging ICT service providers to voluntarily develop and enforce terms of service that target content aimed at recruitment for terrorism and recruiting or inciting others to commit terrorist acts, while respecting international human rights law, and publish regular transparency reports on the implementation of such terms of service and takedown requests from Member States, taking into consideration the work of the industry-led Global Internet Forum to Counter Terrorism and the Tech Against Terrorism initiative led by the Counter-Terrorism Committee Executive Directorate.

223. The following issues should be considered:

(a) Regarding domestic investigations (legislation):

(i) Does national legislation enable the expedited preservation of digital data?

(ii) Does national legislation enable the disclosure of content, traffic data and/or basic subscriber information from an Internet service provider and other ICT firms in an emergency?

(iii) Do national laws include an obligation for Internet service providers and other ICT firms to retain client data for a specified period?[124]

(iv) Do national laws explicitly include a power to obtain basic subscriber information from an Internet service provider or ICT firm?[125]

(v) Do national laws explicitly include a power to obtain traffic data from an Internet service provider or ICT firm?

(vi) Do national laws explicitly include a power to obtain content data from an Internet service provider or ICT firm?

[123] International Covenant on Civil and Political Rights, art. 17.

[124] Global survey of the implementation by Member States of Security Council resolution 1373 (2001) (S/2016/49, annex).

[125] Ibid.

(vii) Do national laws explicitly provide for real-time collection of content data from an Internet service provider or ICT firm?[126]

(viii) Do national laws explicitly provide for real-time collection of traffic data from an Internet service provider or ICT firm?

(ix) Do national laws explicitly empower the competent authorities to order a person or entity on its territory to produce any data under its possession or control?[127]

(x) Does national legislation explicitly include a power to access computer hardware or data?[128]

(xi) Do national laws explicitly provide for a power to seize computer hardware or data?[129]

(xii) Must a search and seizure of computer hardware or data be undertaken by an expert?

(xiii) Do national laws explicitly provide for the disclosure of encryption keys?

(xiv) Do national laws explicitly provide that electronic evidence/records are admissible in court proceedings and provide for a process for using authentication rules?[130]

(xv) Does the State ensure respect for the data subjects' right to freedom from arbitrary or unlawful interference with privacy under international law, as well as for relevant protections under national law, which may include access, rectification, restrictions on use and judicial redress?

(b) Regarding national structure, capacity and cooperation:

(i) Has the State developed ICT capacities and expertise within criminal justice and law enforcement agencies?

(ii) Has the State strengthened the capacity of these agencies to monitor social media content relating to terrorism in order to prevent the flow of foreign terrorist fighters, in a manner that is compliant with States' international human rights obligations?

(iii) Are the responsible authorities able to use social media content relating to terrorism as digital evidence for investigation and prosecution, while respecting human rights and fundamental freedoms, consistent with their obligations under domestic and applicable international law?[131]

(iv) What laws, policies and measures has the State put in place to protect the right to freedom of expression and opinion when collecting and disclosing digital data in counter-terrorism investigations?

---

[126] Ibid.

[127] Ibid.

[128] African Union Convention on Cyber Security and Personal Data Protection, art. 31 (3); the Commonwealth Model Law on Computer and Computer Related Crime of 2002, sect. 12; Council of Europe Convention on Cybercrime, art. 19; International Telecommunication Union/Caribbean Community/Caribbean Telecommunications Union, *Cybercrime/E-Crimes: Model Policy Guidelines and Legislative Texts – Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean* (2012), sect. II "Model legislative text – cybercrime/ e-crimes", part IV, sect. 20.

[129] S/2016/49, annex.

[130] Ibid.

[131] Addendum to the Madrid Guiding Principles, guiding principle 44 (d).

(v) Has the State put in place an independent oversight system, consisting of both judiciary mechanisms and other bodies, mandated to ensure the lawful conduct of law enforcement and intelligence agencies in the collection and disclosure of digital data?

(vi) Are the responsible authorities able to handle cases involving incitement to commit terrorist acts and terrorist recruitment when those offences are committed through the Internet?

(vii) Has the State encouraged private companies to establish round-the-clock mechanisms for cooperation with law enforcement and clear rules for the preservation of digital evidence and emergency disclosure requests in accordance with applicable law?[132]

(viii) Is there a national round-the-clock contact point for domestic investigations requiring data from Internet service providers or ICT firms?

(ix) Has a cyber emergency-response team been established?

(c) Regarding cross-border investigations:

(i) Does the State's national legislation enable the competent authorities of the State to directly contact Internet service providers in another State to request the preservation of specified data?

(ii) Does the State's national legislation enable the competent authorities of the State to directly contact Internet service providers in another State to make an emergency request to disclose data?

(iii) Does the State's national legislation enable the competent authorities of the State to directly contact Internet service providers in another State to request basic subscriber information and/or traffic data?

(iv) Does the State's national legislation enable the competent authorities of another State to directly contact Internet service providers in the former State to request the preservation of specified data?

(v) Does the State's national legislation enable the competent authorities of another State to directly contact Internet service providers in the former State to make an emergency request to disclose data?

(vi) Does the State's national legislation enable the competent authorities of another State to directly contact Internet service providers in the former State to request basic subscriber information and/or traffic data?

(vii) Do national laws explicitly provide that electronic evidence/records obtained from another jurisdiction are admissible in court proceedings and provide for a process for using authentication rules?

(viii) Do the relevant national authorities know how to make direct requests to Internet service providers for the preservation of electronic evidence and the voluntary disclosure and emergency disclosure of data?

(ix) Do the responsible authorities know how to draft a mutual legal assistance request to another State for electronic evidence?

(x) Has the State considered ways in which to enhance cooperation between the relevant investigation agencies, including police-to-police mechanisms and

[132] Ibid., guiding principle 44 (b).

with the private sector, especially with Internet service providers, in gathering data and evidence in cases relating to terrorism and foreign terrorist fighters?[133]

(xi) Is there a round-the-clock focal point for both outgoing and incoming international requests for the preservation of data, emergency disclosure of data and the sharing of spontaneous information?

(xii) Does the State have a national guide or manual to assist requesting States making requests for electronic evidence?

(xiii) Have the relevant authorities considered making use of the *Practical Guide for Requesting Electronic Evidence across Borders* developed by the Counter-Terrorism Committee Executive Directorate, UNODC and the International Association of Prosecutors?[134]

(xiv) Are there any model forms for requests for the preservation of data, direct requests and/or emergency disclosure requests to Internet service providers?

(xv) Does the State ensure respect for the data subjects' right to freedom from arbitrary or unlawful interference with privacy under international law, as well as for relevant protections under national law, which may include access, rectification, restrictions on use and judicial redress?

224. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principle 26;

(b) Addendum to the Madrid Guiding Principles, guiding principle 49;

(c) Counter-Terrorism Committee Executive Directorate/UNODC/International Association of Prosecutors, *Practical Guide for Requesting Electronic Evidence across Borders* (2019);

(d) INTERPOL/United Nations Counter-Terrorism Centre of the Office of Counter-Terrorism joint handbook "Using the Internet and social media for counter-terrorism investigations", 2019;

(e) UNODC, *Human Rights and Criminal Justice Responses to Terrorism: Counter-Terrorism Legal Training Curriculum Module 4* (Vienna, 2014), section 2.3;

(f) Office of the United Nations High Commissioner for Human Rights (OHCHR), *Human Rights, Terrorism and Counter-Terrorism: Fact Sheet No. 32* (July 2008), chapter III, sections H and J;

(g) Counter-Terrorism Implementation Task Force, *Guidance to States on Human Rights-Compliant Responses to the Threat Posed by Foreign Fighters* (New York, 2018), chapters VII and X.

(c) Forensic evidence

225. Forensic capacity is an important component, not only of modern criminal investigations, but also of the entire criminal justice system. During the investigative phase, evidence is collected at a crime scene or from a person (e.g., a suspect, victim or witness), analysed by applying scientific methods and presented in a court of law. In the context of a terrorism-related investigation, forensic science can assist prosecutors and investigators in, for instance, linking a person to a specific activity or event, place or material, or to another person. The type of evidence collected and analysed by applying forensics will vary according to the type of offence being

[133] Ibid., guiding principle 44 (e).
[134] Ibid., guiding principle 44 (f).

investigated and may include biological evidence (such as DNA), latent print evidence, digital evidence, ballistics or trace evidence. Likewise, the provision of forensic services will vary according to the type of national legal system.

226. Forensic biometrics (such as fingerprints, DNA and facial) are key components of forensic science and vital elements in law enforcement investigations. These capabilities require the coordinated input of other pertinent disciplines within forensic science and areas of specialist technical and laboratory expertise. The processing of all forensic science material, at the crime scene and in the laboratory, should be conducted in compliance with international standards and associated quality management systems.

227. The following issues should be considered:

(a) Does the police force or relevant law enforcement agency have the capacity to apply forensic science to collect and analyse physical evidence?

(b) Do the police have a dedicated scientific police or forensic science laboratory with access to proper equipment, facilities/laboratories, expertise and training, to process physical evidence?

(c) Has the State built ICT and forensic capacities and expertise within national law enforcement agencies?[135]

(d) Has the State put in place sufficient governance mechanisms, regulations, data protection, privacy policies, risk management and vulnerability assessments in order to collect, process and use forensic evidence, including biometrics, responsibly and properly and in full compliance with international human rights obligations?

(e) Do the responsible authorities use existing good practices and standard operating procedures, including those of INTERPOL, for forensic science procedures, in order to ensure the reliability of forensic evidence in court and promote public confidence?[136]

228. The following international instruments, standards and good practices provide guidance in this area:

(a) *Crime Scene and Physical Evidence Awareness for Non-Forensic Personnel* (United Nations publication, Sales No. E.09.IV.5);

(b) Madrid Guiding Principles, guiding principles 26 and 27;

(c) Addendum to the Madrid Guiding Principles, guiding principles 38 and 43–45;

(d) Office for Disarmament Affairs information hub on improvised explosive devices;[137]

(e) INTERPOL, “Guidelines concerning transmission of fingerprint crime scene marks”, 2012;

(f) INTERPOL, *INTERPOL Handbook on DNA Data Exchange and Practice: Recommendations from the INTERPOL DNA Monitoring Expert Group*, 2nd ed. (2009);

(g) European Network of Forensic Science Institutes, *Best Practice Manual for the Forensic Examination of Digital Technology* (November 2015);

[135] Madrid Guiding Principles, guiding principle 26.
[136] Addendum to the Madrid Guiding Principles, guiding principle 43 (c).
[137] Available at www.un.org/disarmament/convarms/ieds/.

(h) Office for Democratic Institutions and Human Rights of OSCE, *Human Rights in Counter-Terrorism Investigations: A Practical Manual for Law Enforcement Officers* (Warsaw, 2013);

(i) United Kingdom of Great Britain and Northern Ireland, Association of Chief Police Officers, "ACPO good practice guide for computer-based electronic evidence", 2012;

(j) Counter-Terrorism Committee Executive Directorate/Office of Counter-Terrorism, *United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism* (2018);

(d) Information and evidence collected by the military

229. The following issues should be considered:

(a) Does the State work to facilitate the collection, sharing and admissibility of information and evidence related to terrorism and foreign terrorist fighter cases by the military, while preserving the chain of custody and respecting the integrity of the criminal proceedings, limiting such practices to high-risk situations, such as post-conflict or conflict situations in which civilian law enforcement and judicial officials cannot play their role, and in compliance with international human rights law and international humanitarian law?

(b) Do law enforcement officials and prosecutors establish, as early in the process as possible, working relationships and lines of communication with the relevant actors in conflict zones and high-risk situations, operating under a legal mandate to assist in collecting information that can be submitted as evidence?

230. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principles 22–32;

(b) Counter-Terrorism Committee Executive Directorate, "Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences", developed within the framework of the Working Group on Criminal Justice, Legal Responses and Countering the Financing of Terrorism of the United Nations Global Counter-Terrorism Coordination Compact; and Global Counterterrorism Forum, "Abuja recommendations on the collection, use and sharing of evidence for purposes of criminal prosecution of terrorist suspects", 2018.

2. Detention

231. Any form of detention must be carried out in accordance with procedures established by law. Arbitrary detention is impermissible under any circumstances. Although some States have instituted special procedures for extended investigative detention in terrorism-related cases, pretrial detention is nonetheless considered under international human rights law to be the exception rather than the rule. It must not last for prolonged or indefinite periods and must be closely supervised by an independent judicial mechanism. The presumption of innocence has been qualified as a non-derogable right.

232. In its resolution 2396 (2017), the Council notes that prisons can serve as potential incubators for radicalization to terrorism and terrorist recruitment, as well as spaces for the rehabilitation and reintegration of prisoners. (For more information on this issue, see also chapter II, section K, "Prosecution, rehabilitation and reintegration".)

233. The following issues should be considered:

(a) Has the State instituted special procedures allowing for extended investigative detention in terrorism-related cases?

(b) Is detention subject to prompt and periodic review by an independent and impartial tribunal?

(c) Does the State assure the accused the right to prepare an effective defence, including meaningful access to counsel?

(d) Does the State have in place special provisions for extended or indefinite administrative detention without trial? How have international human rights mechanisms assessed such arrangements?

3. Prosecution

234. The Counter-Terrorism Committee has recognized that the prosecution of terrorists has become increasingly complex and highly specialized. Prosecutors need to know typologies of incitement and of recruitment, and they need specialization, an understanding of charity laws, finance, ICT and methods of work of terrorist organizations, as well as an understanding of the range of special investigative techniques available. This process requires a degree of training, knowledge, skill and sophistication. They need to be able to guide, instruct and supervise the work of the investigatory agencies. The present guide incorporates a number of recommendations to assess the practical elements of effective implementation for the prosecution and judiciary.

235. In order to be able to bring terrorists to justice, States must put in place an effective prosecution system. The State's prosecution system must have the capacity and expertise to correctly seek mutual legal assistance and extradition requests and to effectively cooperate with the State central authority or, as appropriate, other relevant criminal justice authorities in order to prevent, investigate and prosecute terrorist acts.

236. In its resolution 2396 (2017), the Council calls upon States to consider prosecution, rehabilitation and reintegration measures. (For more information on this issue, see also chapter II, section J, "Investigating, prosecuting and adjudicating terrorist acts".)

237. The following issues should be considered:

(a) Does the State's prosecution system have the capacity and expertise to handle complex cases (involving conspiracy, charity law, finance, human rights)?

(b) Has the State established a special prosecutors' unit or designated public prosecutors to deal exclusively with terrorism cases or with serious crimes, including terrorism cases?[138]

(c) Does the State's prosecution system have the capacity and expertise to supervise the use of special investigative techniques by investigative agencies?

(d) Does the State's prosecution system have the capacity and expertise to handle intelligence collected by investigative agencies and convert it, where appropriate, and subject to the arrangements of its legal system, into admissible evidence?

(e) Does the State's prosecution system have the capacity and expertise to handle evidence collected by different States?

[138] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.7.1.

(f) Does the State's prosecution system have access to appropriate training?

(g) Does the State's prosecution system have the capacity to integrate and utilize financial intelligence with other types of information?[139]

(h) Does the State's prosecution system have the capacity and expertise to handle counter-financing of terrorism measures (freezing, confiscation, etc.)?

(i) Does the State's prosecution system have the capacity and expertise to prosecute terrorists benefiting from transnational organized crime and transnational organized criminals working with them[140] and to handle recruitment and incitement offences?

(j) Does the State's prosecution system have the capacity and expertise to consistently update training and evidence collection and special investigative techniques so as to incorporate new ICT?[141]

(k) Does the State's prosecution system have the capacity and expertise to cooperate internationally (formally and informally) on these issues?

(l) Does the State's prosecution system have the capacity and expertise to coordinate action among government agencies, including in the ICT and law enforcement sectors?

(m) Does the State's prosecution system have informal coordination mechanisms between the different sections of a prosecution service, as well as with other agencies (i.e., law enforcement agencies)?

(n) Has the State put in place prosecution approaches that take into account the rights of the child, as defined under international law, and make the best interests of the child a primary consideration?[142] (For more information on children and children's rights, see also chapter IV, section H, "Complying with international human rights, refugee and humanitarian law"; for more information on child-sensitive prosecution, rehabilitation and reintegration strategies, see also chapter II, section K, "Prosecution, rehabilitation and reintegration".)

4. Judiciary

238. In order to be able to bring terrorists to justice, States must put in place an effective judicial system. An approach to terrorism based on the rule of law requires an independent judiciary that is capable of handling the complex requirements of terrorism cases with evidence that may come from intelligence, financial, electronic or military sources. The judiciary may have to protect the sources and methods of the evidence collection while guaranteeing the rights of the accused to fair trial guarantees.

239. The following issues should be considered:

(a) Does the State's court system have the capacity and expertise to handle complex cases (involving conspiracy, charity law, finance, human rights)?

(b) Does the State's court system provide judges with training in forensic, technological and financial aspects of investigation and prosecution?

---

[139] Resolution 2322 (2016).

[140] Ibid., para. 9 (c).

[141] Preliminary analysis of the principal gaps in Member States' capacities to implement Security Council resolutions 1373 (2001) and 1624 (2005) that may hinder their abilities to stem the flow of foreign terrorist fighters pursuant to Security Council resolution 2178 (2014) (S/2014/807, annex).

[142] Addendum to the Madrid Guiding Principles, guiding principles 42, 43 and 47.

(c) Does the State's court system have the capacity and expertise to cooperate internationally (formally and informally)?

(d) Can the State's court system control the use of special investigative techniques by investigative and prosecutorial agencies?

(e) Does the State's court system provide for access to classified or national security information by judges? If so, how are the rights of the accused to fair trial guaranteed?

(f) Does the State's court system have the capacity and expertise to fight transnational crimes that can support or facilitate terrorist activity?

(g) Does the State's court system have sufficient human resources?

(h) Does the State's court system have, where appropriate, access to special gender-sensitive training or educational programmes for judges and courts concerning counter-terrorism, money-laundering and terrorism-financing offences?

(i) Does the State's court system provide training on sentencing specific to terrorism, taking into account issues related to rehabilitation and reintegration?

(j) Does the State's court system provide training on juvenile issues?

(k) Does the judiciary exercise regular and independent oversight of counter-terrorism measures in order to ensure fair treatment and due process?

(a) Special courts and court procedures

240. Some States have conferred jurisdiction on special courts to deal with terrorism-related cases. Some States have also instituted special provisions relating to court procedures, including with respect to forms of evidence that are admissible. In paragraph 22 of its general comment No. 32 (2007) on the right to equality before courts and tribunals and to a fair trial (article 14 of the International Covenant on Civil and Political Rights), the Human Rights Committee reaffirmed that trial of civilians by military courts should be considered exceptional. In accordance with article 10 of the Universal Declaration of Human Rights, everyone is entitled "in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him". Although certain aspects of the right to fair trial may be subject to certain restrictions in exceptional situations, all such measures must be guided by the principles of legality, necessity, proportionality and non-discrimination. The Human Rights Committee has also stated that fundamental requirements of fair trial must be respected in all cases. Public hearings may be limited for reasons of morals, public order or national security in a democratic society, or when the interest of the private lives of the parties so requires, or to the extent strictly necessary in the opinion of the court of special circumstances where publicity would be prejudicial to the interests of justice.[143] However, with respect to cases where the death penalty could be imposed, the Committee has stated that all fair-trial obligations should be respected, due to the non-derogable nature of the right to life.

241. Some States have also chosen to deal with terrorism-related matters through their ordinary criminal procedures. Others have established special procedures on the grounds that terrorism-related cases pose exceptional challenges to law enforcement. Such procedures may include exceptional rules governing detention, evidence and other trial matters, and the establishment of special or military courts. Although such measures may have rational foundations, it is essential to consider whether they comply with the principles of legality, necessity and proportionality and whether they

[143] Human Rights Committee, general comment No. 32, para. 29.

are accompanied by appropriate safeguards. In rare circumstances, States may declare states of exception or emergency, owing to the perceived threat of terrorism. Such actions must be carried out in conformity with applicable international law (including, for States parties, the requirements of article 4 of the International Covenant on Civil and Political Rights).

242. The following issues should be considered:

(a) Are terrorism cases tried by independent judges appointed or elected by normal procedure (i.e., non-military, non-emergency measures)?[144]

(b) Has the State instituted special legal procedures in cases involving terrorism charges? If so, how has it ensured that all human rights obligations are complied with in practice?

(c) In cases in which capital punishment may be imposed, does the State rigorously ensure compliance with all fair-trial obligations?

(d) Are terrorism trials legally guaranteed to be open to the public, in principle?[145]

243. The following international instruments, standards and good practices provide guidance in this area:

(a) Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment;

(b) Basic Principles on the Independence of the Judiciary;

(c) Guidelines on the Role of Prosecutors;

(d) Human Rights Committee, general comment No. 29 (2001) on derogations from provisions of the Covenant during a state of emergency (article 4 of the International Covenant on Civil and Political Rights); general comment No. 32; general comment No. 35 (2014) on liberty and security of person (article 9 of the Covenant);

(e) Reports of the Working Group on Arbitrary Detention of the Human Rights Council;

(f) Madrid Guiding Principles;

(g) Counter-Terrorism Implementation Task Force, *Basic Human Rights Reference Guide: Right to a Fair Trial and Due Process in the Context of Countering Terrorism* (New York, October 2014);

(h) Counter-Terrorism Implementation Task Force, *Basic Human Rights Reference Guide: Detention in the Context of Countering Terrorism* (New York, October 2014);

(i) Counter-Terrorism Implementation Task Force, *Basic Human Rights Reference Guide: Conformity of National Counter-Terrorism Legislation with International Human Rights Law* (New York, October 2014);

(j) The work of the Global Counterterrorism Forum, especially The Hague Memorandum on Good Practices for the Judiciary in Adjudicating Terrorism Offenses and the Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector;

[144] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.7.2.

[145] Ibid., template 2.7.3.

(k) The work of the Office for Democratic Institutions and Human Rights of OSCE, especially *"Countering Terrorism, Protecting Human Rights: A Manual"* (Warsaw, 2007);

(l) The work of the African Centre for Studies and Research on Terrorism, especially the research handbook on international law and terrorism.

(b) Safeguards for criminal justice personnel

244. In many Member States, those involved in the investigation and prosecution of organized crime and terrorism cases are directly exposed to security risks. The ability to participate in law enforcement investigations and/or judicial proceedings without fear of intimidation or reprisal is essential to maintaining a fair and effective criminal justice system.[146] Member States should have programmes in place to protect law enforcement officials, prosecutors, the judiciary and other relevant persons involved in the investigation and prosecution of terrorists.[147]

245. The following issues should be considered:

(a) Is there an appropriate State authority responsible for providing public prosecutors, law enforcement officials, judges, and their families with information, training and advice concerning personal safety?[148]

(b) Has the State criminalized the use of physical force, threats or intimidation to interfere with the exercise of official duties by a justice or law enforcement official?[149]

(c) Is the judiciary able to exercise its judicial function independently on the basis of facts and in accordance with the law, without any restrictions, pressures, threats or interferences?[150]

(d) If prosecutors, judges, law enforcement officials, or their families, are subjected to violence or threats of violence, or are harassed, stalked, intimidated, or coerced in any manner, are there safeguards to ensure that such incidents are fully investigated, that those at risk are informed concerning the outcome of the investigation, that steps are taken to prevent recurrence, and that those at risk and their families receive any necessary counselling or psychological support?[151]

(e) Does the State ensure that public prosecutors, law enforcement officials, judges, together with their families, are physically protected by the appropriate State authorities when their personal security is threatened as a result of a proper discharge of their functions?

(f) Does the State provide the workplace and homes of relevant prosecutors and judges with appropriate security devices and personal protection devices?

(g) Does the State ensure the safety of all stakeholders involved, including victims, civil society actors, women and youth?

---

[146] Guidelines on the Role of Prosecutors, adopted at the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 1990, para. 4; and Global Counterterrorism Forum, Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector, good practice 1.

[147] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.6.7.

[148] International Association of Prosecutors, Declaration on minimum standards concerning the security and protection of public prosecutors and their families, art. 5.

[149] United Nations Convention against Transnational Organized Crime.

[150] Bangalore Principles of Judicial Conduct, value 1, "Independence".

[151] International Association of Prosecutors, Declaration on minimum standards concerning the security and protection of public prosecutors and their families, art. 8 (iv).

246. The following international instruments, standards and good practices provide guidance in this area:

(a) Bangalore Principles of Judicial Conduct, 2002, adopted by the Judicial Group on Strengthening Judicial Integrity and endorsed by UNODC;

(b) International Association of Prosecutors, Declaration on minimum standards concerning the security and protection of public prosecutors and their families.

(c) Security and safety in the courtroom

247. In order to be able to bring terrorists to justice, Member States should ensure the safety and security of the courtrooms so that judges, witnesses, victims, law enforcement officials and prosecutors will not be subject to intimidation, hindrance, harassment, improper interference or unjustified exposure to civil, criminal or other liability.[152]

248. The following issues should be considered:

(a) Does the State ensure the presence of security guards or police protection for judges who may become, or are, victims of serious threats?[153]

(b) Has the State considered putting in place an increased police or other security presence, both in and outside the courtroom?

(c) Has the State considered the use of security checkpoints and screening procedures, metal detectors, X-ray scanning devices and other screening technology at public entrances to courthouses and courtrooms?

(d) Has the State considered prohibiting the possession (or use) of cell phones and other electronic devices in the courthouse and courtroom?

(e) Has the State considered separate and secure parking entrances for judges, prosecutors and court personnel?[154]

249. The following international instruments, standards and good practices provide guidance in this area:

(a) UNODC, *The Status and Role of Prosecutors: A United Nations Office on Drugs and Crime and International Association of Prosecutors Guide*, Criminal Justice Handbook Series (New York, 2014);

(b) Council of Europe, *Judges: Independence, Efficiency and Responsibilities – Recommendation CM/Rec(2010)12 and Explanatory Memorandum* (November 2011);

(c) International Association of Prosecutors, Declaration on minimum standards concerning the security and protection of public prosecutors and their families;

(d) Global Counterterrorism Forum, The Hague Memorandum on Good Practices for the Judiciary in Adjudicating Terrorism Offenses.

[152] Guidelines on the Role of Prosecutors, para. 4.

[153] Recommendation No. R (94) 12 of the Committee of Ministers of the Council of Europe to member States on the independence, efficiency and role of judges, adopted on 13 October 1994 at the 518th meeting of the Ministers' Deputies, principle III, para. 2.

[154] Global Counterterrorism Forum, The Hague Memorandum on Good Practices for the Judiciary in Adjudicating Terrorism Offenses.

(d) Witness protection

250. In some areas of criminality, including terrorism, there is an increasing risk that witnesses will be subjected to intimidation. States should therefore provide protection to witnesses and to collaborators of justice.

251. The following issues should be considered:

(a) Does the State provide physical and social protection to witnesses and collaborators of justice and people close to them before, during and after the testimony is given, as the case merits?

(b) Does the State allow the admissibility of evidence while permitting, where appropriate, non-disclosure of, or limitations on the disclosure of, information concerning the identity and whereabouts of such witnesses? How does it safeguard the rights of the defence in such cases?

(c) Has the State developed a witness protection programme that includes an autonomous agency, with sufficient resources, able to deal with urgent cases while also guaranteeing the confidentiality of the witness?

(d) Has the State developed international cooperation arrangements in order to provide protection to witnesses, where appropriate, and to enable them to give their testimony in a secure location?

(e) Does the State provide adequate training to criminal justice personnel, develop guidelines to deal with cases in which witnesses might require protection measures or programmes, and ensure adequate resourcing of such measures and programmes?

(e) Rights of victims in criminal proceedings

252. The Council has expressed profound solidarity with the victims of terrorism and their families and has encouraged the Counter-Terrorism Committee Executive Directorate to take into account the important role that victims and survivor networks play in countering terrorism.[155] Acknowledgement of victims of terrorism in criminal proceedings is an important part of recognizing the humanity of the victims, thereby publicly reinforcing the human costs of terrorism.

253. Victims are essential in the investigation and prosecution of acts of terrorism. They often serve as important witnesses in investigations and trials. Legal procedures and practical measures should be in place to protect them.[156] The ability to participate without fear of intimidation or reprisal is essential to maintaining the rule of law[157] and strengthens the ability of States to bring terrorists to justice.

254. Women and girls are often directly targeted by terrorist groups and subjected to gender-based violence, including in the form of rape, forced prostitution, forced marriage, forced pregnancy and human trafficking. The Council stresses that acts of trafficking in persons and sexual and gender-based violence in conflict can be part of the strategic objectives and ideology of, and used as a tactic by, certain terrorist groups, by, inter alia, incentivizing recruitment; supporting financing through the sale and trade of and trafficking in women, girls and boys; destroying, punishing, subjugating or controlling communities; displacing populations from strategically important zones; extracting information for intelligence purposes from male and female detainees; and advancing ideology that includes the suppression of women's

[155] Resolution 2129 (2013), para. 16.

[156] Madrid Memorandum on Good Practices for Assistance to Victims of Terrorism Immediately after the Attack and in Criminal Proceedings, good practice 9.

[157] Ibid.

rights and the use of religious justification to codify and institutionalize sexual slavery and exert control over women's reproduction.[158]

255. The Council has affirmed that victims of trafficking in persons in all its forms, and of sexual violence, committed by terrorist groups should be classified as victims of terrorism with the purpose of rendering them eligible for official support, recognition and redress available to victims of terrorism, having access to national relief and reparations programmes, contributing to lifting the sociocultural stigma attached to this category of crime, and facilitating rehabilitation and reintegration efforts.[159]

256. The following issues should be considered:

(a) Does the State have adequate safeguards and security measures in place to ensure the protection of victims' rights to life, physical security and privacy?[160]

(b) Does the State have a support system in place to assist victims of terrorism and their families throughout the criminal justice process?[161]

(c) Does the State allow for the participation of victims or their next of kin in proceedings against the perpetrator?[162]

(d) Has the State implemented a legal framework establishing rights and roles for victims during the criminal justice process?[163]

(e) Does the State provide for the interpretation of information related to the investigation or criminal proceedings?[164]

(f) Does the State prevent secondary and repeat victimization within the criminal justice process by providing sensitivity training (including gender sensitivity) to judges and other participants in the criminal justice system?[165]

(g) Does the State classify victims of trafficking in persons and sexual violence committed by terrorist groups as victims of terrorism so as to render them eligible for official support, recognition and redress available to victims of terrorism?

257. The following international instruments, standards and good practices provide guidance in this area:

(a) UNODC, *The Criminal Justice Response to Support Victims of Acts of Terrorism* (Vienna, 2012);

(b) Global Counterterrorism Forum, Madrid Memorandum on Good Practices for Assistance to Victims of Terrorism Immediately after the Attack and in Criminal Proceedings;

(c) Shanghai Cooperation Organization Convention against Terrorism, article 7 (8).

---

[158] Resolution 2331 (2016), para. 8.

[159] Ibid., para. 10.

[160] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: framework principles for securing the human rights of victims of terrorism (A/HRC/20/14), para. 67 (g).

[161] Ibid., para. 37.

[162] Ibid., para. 39.

[163] Madrid Memorandum on Good Practices for Assistance to Victims of Terrorism Immediately after the Attack and in Criminal Proceedings, good practice 3.

[164] A/HRC/20/14, para. 40.

[165] Madrid Memorandum on Good Practices for Assistance to Victims of Terrorism Immediately after the Attack and in Criminal Proceedings, good practice 15.

5. Cases involving children

258. Has the State put in place special safeguards and legal protections to ensure that appropriate action is taken in cases involving children, in full compliance with their obligations under international law, ensuring that the competent authorities:

(a) Fully respect and promote the rights of the child, taking into account the best interests of the child as a primary consideration;

(b) Take into consideration the age of the child and the many roles in which children associated with foreign terrorist fighters may have served, while recognizing that such children may be victims of terrorism;

(c) Consider the impact of terrorism on children and children's rights, especially with regard to issues relating to the families of returning and relocating foreign terrorist fighters;

(d) Assess each child individually and without prejudice, and take his or her rights and needs into account, while also considering the circumstances relating to the case and proceeding with any further criminal or security-related actions;

(e) Are provided with appropriate scope for discretion at all stages of proceedings and have at their disposal a variety of alternatives to judicial proceedings and sentencing, including (if appropriate) age-sensitive child protection measures;

(f) Are provided with clear guidelines with respect to whether, or under what conditions, they should keep a child in detention and in which cases diversion is possible, subject to regulation and review, in accordance with international law and domestic standards, and bearing in mind that, in cases involving children, detention should be used as measure of last resort;

(g) Act in accordance with the guidelines regulating pretrial detention and the utilization of other measures of restraint, as provided for in their criminal legislation and defined in compliance with international law?

259. The following international instruments, standards and good practices provide guidance in this area:

(a) Addendum to the Madrid Guiding Principles, guiding principle 42;

(b) Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights;

(c) Johannesburg Principles on National Security, Freedom of Expression and Access to Information;

(d) Human Rights Council resolution 32/13 on the promotion, protection and enjoyment of human rights on the Internet.

K. Prosecution, rehabilitation and reintegration

260. In paragraph 4 of its resolution 2178 (2014), the Council calls upon States, in accordance with their obligations under international law, to cooperate in efforts to address the threat posed by foreign terrorist fighters, including by developing and implementing prosecution, rehabilitation and reintegration strategies for returning foreign terrorist fighters.

261. In its resolution 2396 (2017), the Council calls upon States to assess and investigate suspected individuals whom they have reasonable grounds to believe are terrorists, including suspected foreign terrorist fighters and their accompanying family members, including spouses and children, entering those States' territories, to

develop and implement comprehensive risk assessments for those individuals, and to take appropriate action, including by considering appropriate prosecution, rehabilitation and reintegration measures, and emphasizes that States should ensure that they take all such action in compliance with domestic and international law.

262. In guiding principle 30 of the Madrid Guiding Principles, the Counter-Terrorism Committee notes that Member States should ensure that their competent authorities are able to apply a case-by-case approach to returnees, on the basis of risk assessment, the availability of evidence and related factors. Member States should develop and implement strategies for dealing with specific categories of returnees, in particular minors, women, family members and other potentially vulnerable individuals. Prosecution strategies should correspond to national counter-terrorism strategies, including effective strategies to counter violent extremism. In guiding principle 31, the Committee notes that Member States should consider appropriate administrative measures and/or rehabilitation and reintegration programmes as alternatives to prosecution in appropriate cases. Such measures should be used in a manner compliant with applicable international human rights law and national legislation and should be subject to effective review. In the addendum to the Madrid Guiding Principles, the Committee provides additional guidance on developing and implementing prosecution, rehabilitation and reintegration strategies and protocols, including in cases involving children (see guiding principles 46 and 47).

263. In developing and implementing prosecution, rehabilitation and reintegration strategies, two main issues should be taken into consideration. First, resolution 2178 (2014) requires Member States to "ensure that their domestic laws and regulations establish serious criminal offences sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness" of the foreign terrorist fighter-related offences listed in paragraph 6 of the resolution. In combating the foreign terrorist fighter threat, it is important to address the full range of serious crimes committed during travel, in particular war crimes, crimes against humanity and gender-related crimes.[166] In paragraph 7 of its resolution 2331 (2016), the Council urges all States to ensure that their domestic laws and regulations establish serious criminal offences sufficient to provide the ability to prosecute and penalize in a manner duly reflecting the seriousness of the offence of trafficking in persons committed with the purpose of supporting terrorist organizations or individual terrorists, including through the financing of and recruitment for the commission of terrorist acts.

264. Assessments should be conducted to determine the level of culpability and thereby determine the appropriate way to handle each individual.[167] Whether rehabilitation and reintegration programmes can be introduced during differing stages of criminal proceedings as an alternative to incarceration or in addition to incarceration, including as part of a reduced sentence, depends on the national legislation and criminal justice system of each State. Second, prosecution, rehabilitation and reintegration strategies must comply with applicable international human rights law and humanitarian law, as well as with domestic law, including in cases where rehabilitation and reintegration programmes are used as alternatives in different stages of criminal proceedings, and also, on a voluntary basis, in cases where returning foreign terrorist fighters have been acquitted, charges have been dropped, or where the case does not meet the threshold for prosecution, whether due to lack of evidence or because of the age of the offender or other individual considerations. Women and children associated with foreign terrorist fighters returning and relocating from conflict may require special focus and assistance, as they may have served in

[166] Madrid Guiding Principles, guiding principle 32.
[167] Ibid., pp. 19 and 20.

many different roles, including as supporters, facilitators or perpetrators of terrorists acts, and may be victims of terrorism.[168] States should pay particular attention to ensuring that their domestic legislation respects international law with regard to women and children, as well as taking into account the best interests of the child as a primary consideration.

265. The following issues should be considered:[169]

(a) Has the State implemented all its obligations to ensure that terrorists are brought to justice, as required under resolutions 1373 (2001), 2178 (2014) and 2396 (2017), and to ensure that their criminal justice systems are capable of dealing with all serious crimes that may have been committed by foreign terrorist fighters?

(b) Do prosecution, rehabilitation and reintegration strategies correspond to national counter-terrorism strategies, including effective methods to counter violent extremism conducive to terrorism?

(c) Are prosecution, rehabilitation and reintegration measures timely, appropriate, comprehensive and tailored, taking into account gender and age sensitivities and related factors, comprehensive risk assessments, the severity of the crime(s) committed, available evidence, intent and individual culpability, the support network, the public interest and other relevant considerations or factors, as appropriate, and are they in compliance with domestic and international law, including international human rights and humanitarian law?

(d) Can prosecution, rehabilitation and reintegration strategies be combined with other measures, such as monitoring and/or reporting, supervision, probation, fixed addresses, restraining orders, surrender of passport and/or identification and travel bans? Are such measures used in a manner compliant with applicable international human rights law and national legislation and are they subject to effective review?

(e) Has the State considered pursuing a whole-of-government approach, while recognizing the role that can be played by civil society organizations, including in the health, social welfare and education sectors and in local communities, as appropriate? In developing such an approach, States should consider ways to ensure effective coordination and clear leadership, including by creating multidisciplinary teams, which may include law enforcement agencies, the criminal justice sector, prison and probation services, social services and, as appropriate, civil society organizations.

(f) Has the State considered providing actors who assist them in implementing prosecution, rehabilitation and reintegration strategies with the necessary resources, support, guidance and effective oversight and the opportunity to consult with the competent authority, as appropriate?

(g) Does the State engage proactively with civil society when developing rehabilitation and reintegration strategies for returning and relocating foreign terrorist fighters and their families, as civil society organizations may have relevant knowledge of, access to and engagement with local communities?

(h) Has the State considered encouraging the voluntary participation and leadership of women in the design, implementation, monitoring and evaluation of strategies for addressing returning and relocating foreign terrorist fighters and their families?

(i) What measures has the State taken to ensure that programmes aimed at addressing and countering terrorist narratives, including in prisons, respect

[168] Resolution 2396 (2017), para. 31.

[169] Addendum to the Madrid Guiding Principles, guiding principles 46 and 47.

international human rights law, including the right to freedom of opinion and expression, the right to freedom of religion or belief and the right to be free from arbitrary or unlawful interference with privacy?

(j) Has the State undertaken any efforts to monitor, evaluate and review the effectiveness of prosecution, rehabilitation and reintegration strategies?

(k) In cases involving children, does the State ensure that the prosecution, rehabilitation and reintegration strategy:

(i) Makes the best interests of the child a primary consideration?

(ii) Is implemented in full compliance with criminal legislation, taking into account the gravity of any crime that may have been committed, while considering the age of the child and recognizing that such child may also be a victim of terrorism?

(iii) Includes access to health care, psychosocial support and education programmes that contribute to the well-being of children, and grants access to regular education whenever possible?

(iv) Takes into account age and gender sensitivities?

(v) Enables the involvement of child protection actors and the social sector, as well as their effective coordination with the justice sector?

266. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, in particular guiding principles 30–32;

(b) Addendum to the Madrid Guiding Principles, guiding principles 46 and 47;

(c) United Nations, “United Nations common approach to justice for children”, 2008 (in particular, the strategic interventions);

(d) United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules) (General Assembly resolution 70/175, annex);

(e) United Nations Standard Minimum Rules for Non-custodial Measures (the Tokyo Rules) (General Assembly resolution 45/110, annex);

(f) Basic principles on the use of restorative justice programmes in criminal matters (Economic and Social Council resolution 2002/12, annex);

(g) United Nations Rules for the Protection of Juveniles Deprived of their Liberty (General Assembly resolution 45/113, annex);

(h) United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules) (General Assembly resolution 40/33, annex);

(i) United Nations Rules for the Treatment of Women Prisoners and Non-custodial Measures for Women Offenders (the Bangkok Rules) (General Assembly resolution 65/229, annex);

(j) Convention on the Rights of the Child, article 37;

(k) Committee on the Rights of the Child, general comment No. 24 (2019) on children’s rights in the child justice system;

(l) International Covenant on Civil and Political Rights, articles 9 and 14;

(m) UNODC, *Handbook on the Management of Violent Extremist Prisoners and the Prevention of Radicalization to Violence in Prisons* (New York, 2016);

(n) Council of Europe, *Council of Europe Handbook for Prison and Probation Services regarding Radicalization and Violent Extremism* (Strasbourg, December 2016);

(o) European Commission, Radicalization Awareness Network declaration of good practices for engagement with foreign fighters for prevention, outreach, rehabilitation and reintegration.

L. Addressing the risks of terrorist radicalization and recruitment in prisons and ensuring that prisons can serve to rehabilitate and reintegrate prisoners

267. In its resolution 2396 (2017), the Council notes that prisons can serve as potential incubators for radicalization to terrorism and terrorist recruitment, and that proper assessment and monitoring of imprisoned foreign terrorist fighters, aimed at reducing opportunities for terrorists to attract new recruits, is therefore critical. The Council recognizes that prisons can also serve to rehabilitate and reintegrate prisoners, where appropriate, and that Member States may need to continue to engage with offenders after their release from prison in order to prevent recidivism, in accordance with relevant international law and taking into consideration, where appropriate, the United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules). Member States are encouraged to take all appropriate actions to prevent inmates who have been convicted of terrorism-related offences from radicalizing to violence other prisoners with whom they may come into contact, in compliance with domestic and international law.

268. Stand-alone intervention programmes are less likely to be successful in the absence of broader efforts to ensure effective management of all prisoners. Such efforts should include implementing appropriate security measures, intelligence systems and control systems, as well as cooperation with other law enforcement and criminal justice agencies, specialized staff, faith professionals, therapists, mentors and families, as appropriate. All efforts to address the risks of terrorist radicalization and recruitment in prisons and to rehabilitate and reintegrate prisoners must be undertaken in full compliance with national legislation and with relevant international law and should ensure full respect for human rights and fundamental freedoms, including the freedom of opinion and expression, the freedom of religion or belief, the right to be free from arbitrary or unlawful interference with privacy, and the absolute prohibition of torture. Such efforts should also include a gender perspective and take into consideration the needs and rights of children.[170]

269. The following issues should be considered:

(a) Do the responsible authorities ensure proper initial separation of prisoners according to their legal status (pre-trial from convicted), age (children from adults) and gender?

(b) Do the responsible authorities conduct proper intake and regular risk and needs assessments, which inform prisoners' classification and allocation?

(c) Does the State ensure that conditions of detention respect the dignity of all prisoners, including protection from torture and other cruel, inhuman or degrading treatment or punishment; provide adequate material conditions and personal safety; and establish mechanisms to ensure that arrests of suspects and all forms of deprivation of liberty are in accordance with national legislation, as well as with the relevant obligations under international law?

[170] Addendum to the Madrid Guiding Principles, guiding principle 49.

(d) Has the State established a structured prison intelligence system, consistent with national legislation?

(e) Has the State ensured a sufficient number of qualified and well-trained staff, including appropriate specialized staff and other experts, such as faith professionals, therapists and mentors, and established mechanisms and protocols to ensure that all prison staff meet high standards of professional and personal conduct at all times?

(f) Are the relevant programmes aimed at addressing the risks of terrorist radicalization and recruitment in prisons and ensuring that prisons can serve to rehabilitate and reintegrate prisoners based on a clear and consistent understanding of the process of terrorist radicalization and disengagement? Where appropriate, do such programmes have clear, well-defined and, ideally, measurable goals and objectives for disengagement processes?

(g) Has the State put in place a variety of such programmes, including gender- and age-appropriate programmes, which can be targeted to address the specific needs of each individual, combined with access to vocational training and education programmes, as well as religious, creative, cultural and recreational activities, as appropriate?

(h) Has the State established mechanisms for collaboration among prison staff, local community-based service providers, civil society and families, as appropriate?

(i) Has the State considered offering pre-release programmes that provide opportunities for qualified inmates to access local community resources, including work, education and vocational training release programmes, temporary home furlough and local community corrections, as appropriate?

(j) Has the State considered establishing appropriate post-release administrative measures, monitoring and reporting obligations, intervention and support programmes, and protective measures upon release, as appropriate and in accordance with international law, including international human rights law?

(k) Has the State established effective oversight mechanisms, taking into consideration, where, appropriate, the United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules)?

(l) Has the State considered developing gender-sensitive counter-narrative strategies in the prison system?[171]

270. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, in particular guiding principles 30–32;

(b) Addendum to the Madrid Guiding Principles, guiding principle 48;

(c) United Nations, “United Nations common approach to justice for children”, 2008 (in particular, the strategic interventions);

(d) United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules) (General Assembly resolution 70/175, annex);

(e) United Nations Standard Minimum Rules for Non-custodial Measures (the Tokyo Rules) (General Assembly resolution 45/110, annex);

[171] Resolution 2396 (2017), para. 40.

(f) Basic principles on the use of restorative justice programmes in criminal matters (Economic and Social Council resolution 2002/12, annex);

(g) United Nations Rules for the Protection of Juveniles Deprived of their Liberty (General Assembly resolution 45/113, annex);

(h) United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules) (General Assembly resolution 40/33);

(i) United Nations Rules for the Treatment of Women Prisoners and Non-custodial Measures for Women Offenders (the Bangkok Rules) (General Assembly resolution 65/229, annex);

(j) Convention on the Rights of the Child, article 37;

(k) Committee on the Rights of the Child, general comment No. 24 (2019) on children's rights in the child justice system;

(l) International Covenant on Civil and Political Rights, articles 9 and 14;

(m) UNODC, *Handbook on the Management of Violent Extremist Prisoners and the Prevention of Radicalization to Violence in Prisons* (New York, 2016);

(n) European Commission, Radicalization Awareness Network declaration of good practices for engagement with foreign fighters for prevention, outreach, rehabilitation and reintegration;

(o) International Institute for Justice and Rule of Law, "Prison management recommendations to counter and address prison radicalization", recommendations 10–13.

M. Jurisdiction and *aut dedere aut judicare*

271. Pursuant to paragraph 2 (e) of resolution 1373 (2001), the Council requires 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. In paragraph 2 of resolution 1566 (2004), the Council calls upon States to bring such individuals to justice on the basis of the principle to extradite or prosecute (*aut dedere aut judicare*). However, it is extremely difficult to secure the conviction of arrested persons if all the witnesses and the evidence are abroad. Member States should therefore consider revising laws so that nationality or citizenship is not a basis to deny extradition.[172]

272. In its resolution 1624 (2005), the Council recalls that all States must cooperate fully in the fight against terrorism, in accordance with their obligations under international law, in order to find, deny safe haven and bring to justice, on the basis of the principle of extradite or prosecute, any person who supports, facilitates, participates or attempts to participate in the financing, planning, preparation or commission of terrorist acts or provides safe havens.

273. The international counter-terrorism instruments call on States to establish territorial jurisdiction over offences if such offences are committed within their territory or by their nationals (see also chapter III, section C, "Ratifying the international counter-terrorism instruments"). States must also establish jurisdiction over the offences to either prosecute or extradite an alleged offender present in the territory of the State.[173]

[172] S/2015/975, annex, para. 34.

[173] Counter-Terrorism Committee Executive Directorate, "Technical guide to the implementation of

274. The following issues should be considered:

(a) Has the State established its jurisdiction over terrorism offences committed by its own nationals, regardless of the location of the offences committed?[174]

(b) Has the State established its jurisdiction over terrorism offences committed in its territory and on board aircraft and vessels registered in the State?[175]

(c) In the event that the State does not extradite a terrorist, does the State, without exception and regardless of whether or not the terrorism offence was committed in its territory, submit the case without undue delay to its competent authorities for the purpose of prosecution, through proceedings in accordance with its laws, provided that the alleged offence falls within the scope of the international counter-terrorism instruments?[176]

(d) Does the State effectively implement the extradite or prosecute principle, including by implementing the measures set forth in resolution 2322 (2016) concerning extradition?

(e) Does national legislation provide jurisdiction over misuse of cyberspace for terrorist purposes?

N. International legal cooperation

275. Pursuant to resolution 1373 (2001), States are required to undertake a number of measures for the purpose of international legal cooperation in the fight against terrorism. Member States shall provide one another the greatest measure of assistance in the prosecution of acts of terrorism, wherever they occur.[177] In paragraph 12 of its resolution 2178 (2014), the Council recalls resolution 1373 (2001), paragraph 2 (f), in which it calls on States to afford one another the greatest measure of assistance, specifically with respect to such investigations or proceedings involving foreign terrorist fighters.[178]

276. Member States should also afford one another assistance in obtaining evidence in their possession necessary for criminal proceedings.[179] States should therefore consider establishing appropriate laws and mechanisms to allow for the broadest possible international judicial cooperation[180] and to provide more efficient and more effective cooperation.[181] Member States should also dedicate the resources necessary to make existing international cooperation mechanisms effective.[182] States should be aware of, and strengthen their responses to, the numerous challenges associated with effective international cooperation in combating terrorism, including time involved in the provision of mutual legal assistance, procedural rigidities and lack of capacity.[183]

Security Council resolution 1373 (2001)", 2009, chap. II, sect. 8, "Jurisdiction".

[174] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.8.1.

[175] Ibid., template 2.8.2.

[176] Ibid., template 2.9.3.

[177] Resolution 1456 (2003), annex, para. 2 (b).

[178] See also resolution 2133 (2014), para. 5; and resolution 2253 (2015), para. 12.

[179] Resolution 1373 (2001), para. 2 (f).

[180] Resolution 2322 (2016), para. 15.

[181] S/2015/975, annex, para. 31.

[182] Ibid., annex, para. 44.

[183] S/2016/501, para. 52.

277. In its resolution 2322 (2016), the Council calls on all States to undertake a number of additional measures aimed at strengthening mutual legal assistance and extradition, including considering strengthening and, where appropriate, reviewing the possibilities for enhancing the effectiveness of their respective bilateral and multilateral treaties concerning extradition and mutual legal assistance in criminal matters related to counter-terrorism; cooperating, as appropriate, on the basis of reciprocity or on a case-by-case basis; enacting and, where appropriate, reviewing and updating extradition and mutual legal assistance laws, as well as their respective bilateral and multilateral treaties concerning mutual legal assistance and extradition, in connection with terrorism-related offences, consistent with their international obligations, including their obligations under international human rights law; considering ways to simplify extradition and mutual legal assistance requests while recognizing the need for due consideration, in the light of the need to uphold relevant legal obligations; designating central authorities or other relevant criminal justice authorities to handle mutual legal assistance and extradition matters and ensuring that such authorities have adequate resources, training and legal authority, in particular for terrorism-related offences; updating current practices on mutual legal assistance regarding acts of terrorism, including considering, where appropriate, the use of electronic transfers of requests to expedite proceedings, with full respect for existing treaty obligations; considering submitting to the UNODC repository database contact information and other relevant details of designated authorities; and considering developing and participating in regional mutual legal assistance cooperation platforms and developing and enhancing arrangements for expeditious cross-regional cooperation in respect of terrorism-related offences.

278. In its resolution 2396 (2017), the Council calls upon Member States to improve international, regional and subregional cooperation, if appropriate through multilateral and bilateral agreements, to prevent the undetected travel of foreign terrorist fighters from or through their territories, especially returning and relocating fighters, including through increased sharing of information for the purpose of identifying such individuals, the sharing and adoption of best practices, and improved understanding of the patterns of travel by fighters and their families, and for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources to support terrorist acts, while respecting human rights and fundamental freedoms and consistent with their obligations under domestic and applicable international law.

279. International judicial cooperation in cases relating to foreign terrorist fighters, including returnees, relocators and their families, remains a challenge. Recognizing the persisting challenges common to foreign terrorist fighter-related cases, the Council underlines, in its resolutions 2322 (2016) and 2396 (2017), the importance of strengthening international cooperation to prevent, investigate and prosecute terrorist acts.

1. Extradition issues for consideration

(a) Legal framework

280. The following issues should be considered:

(a) Does the State have in place a legal framework covering extradition (acts of parliament, bilateral and multilateral treaties, international counter-terrorism instruments, regional and subregional agreements)?

(b) Has the State enacted and, where appropriate, reviewed and updated extradition and mutual legal assistance laws in connection with terrorism-related

offences, consistent with its international obligations, including its obligations under international human rights law?[184]

(c) Has the State reviewed and updated as necessary its national mutual legal assistance laws and mechanisms in order to strengthen their effectiveness, especially in the light of the substantial increase in the volume of requests for digital data?[185]

(d) Is the State able to use applicable international instruments to which it is a party as a basis for extradition in terrorism cases?[186]

(e) Is the State able to cooperate on the basis of reciprocity or on a case-by-case basis, in the absence of applicable conventions or provisions?[187]

(f) Is the legislative framework sufficiently broad to cover the obligations under resolution 1373 (2001), with respect in particular to the codification of offences and jurisdictional elements such as the principle *aut dedere aut judicare*?

(g) Are the extraditable offences clearly defined in legislation or by reference to applicable treaties?

(h) Does the State impose impediments to extradition where both States have criminalized the underlying conduct?

(i) Are the offences set forth in the international counter-terrorism instruments or required under resolutions 1373 (2001) and 2178 (2014) to be included as extraditable offences in any extradition treaty existing between the contracting States?

(j) Does the State have in place legal provisions requiring denial of extradition requests made by foreign jurisdictions where there are substantial grounds for believing the person concerned would be in danger of being subjected to torture?[188]

(k) Does the State provide for appeal or review of decisions to extradite?

(l) Does the State's legal framework include grounds for refusal such as:

(i) Double jeopardy?

(ii) Improper grounds for prosecution?[189]

(iii) Risk of refoulement under international human rights or refugee law?

(iv) Absence of minimum guarantees in criminal proceedings?

(v) For States that have not abolished the death penalty, absence of adequate guarantees?

(b) Practical application

281. Whereas multilateral and bilateral treaties provide the basis for extradition, domestic legislation and institutions often set out the related procedural aspects. In paragraph 13 (a) of its resolution 2322 (2016), the Council calls on all States to use applicable international instruments to which they are parties as a basis for mutual legal assistance and, as appropriate, for extradition in terrorism cases, and encourages

[184] Resolution 2322 (2016), para. 13 (b).
[185] Ibid., para. 13 (b).
[186] Ibid., para. 13 (a).
[187] Ibid., para. 13 (a).
[188] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.9.11.
[189] See, for example, the International Convention for the Suppression of the Financing of Terrorism, art. 15.

States, in the absence of applicable conventions or provisions, to cooperate, where possible, on the basis of reciprocity or on a case-by-case basis.

282. Review whether a State has established practices, procedures and criteria relating to extradition.

283. The following issues should be considered:

(a) Has the State designated central authorities or other relevant criminal justice authorities to handle mutual legal assistance and extradition matters?[190]

(b) Has the State ensured that such authorities have adequate resources, training and legal authority, in particular for terrorism-related offences?[191]

(c) Does the State provide UNODC with information for its repository database of existing networks of central authorities responsible for counter-terrorism matters, including contacts and other relevant details of designated authorities?[192]

(d) Is there a clear procedure to be followed upon the acceptance of a request for extradition?

(e) Has the State taken steps to strengthen implementation, and where appropriate, review possibilities for enhancing the effectiveness of its bilateral and multilateral treaties concerning extradition in criminal matters related to counter-terrorism?[193]

(f) Has the State considered, within the framework of the implementation of existing applicable international legal instruments, ways to simplify extradition and mutual legal assistance requests in appropriate terrorism-related cases, while upholding relevant legal obligations, including the need for due consideration?[194]

(g) Is there available written information concerning the procedures, which can be provided to requesting States to facilitate extradition?

(h) Are there procedures in place for the arrest of the individual?

(i) Are procedures in place for appeal or judicial review?

(j) Is return prohibited where there are "substantial grounds for believing" that the subject of an extradition request would be in danger of being subjected to torture if returned to his/her State of origin, or any other State?

(k) Is the State able to transmit the items of evidence in its possession to the prosecuting State, in the case of a State refusing extradition?[195]

(l) Have there been extraditions for terrorism-related cases or other cases?

2. Mutual legal assistance

284. Has the State implemented legislation authorizing a competent authority to:

(a) Assist in ensuring the availability of detained persons or others to give evidence or assist in investigations?

(b) Effect service of judicial documents?

---

[190] Resolution 2322 (2016), para. 13 (e).
[191] Ibid., para. 13 (e).
[192] Addendum to the Madrid Guiding Principles, guiding principle 49 (c).
[193] Resolution 2322 (2016), para. 13 (c).
[194] Ibid., para. 13 (d).
[195] UNODC, *Manual on International Cooperation in Criminal Matters related to Terrorism* (New York, 2009), module 1.C.1., p. 30.

(c) Execute searches and seizures?

(d) Examine objects and sites?

(e) Provide information and evidentiary items?

(f) Enhance the coordination of joint investigations?[196]

(g) Provide documents and records, including bank, financial, corporate or business records in admissible form for use in criminal judicial proceedings?

(h) Conduct searches and seizures of information, documents or evidence (including financial records) from financial institutions or other natural or legal persons?

(i) Take evidence or statements from persons?

(j) Facilitate the voluntary appearance of persons for the purpose of providing information or testimony to the requesting State?

(k) Provide unsolicited information to or exchange information with foreign counterparts?[197]

(l) Identify, freeze, seize or confiscate assets used for, or intended to be used for, terrorism financing, as well as the instrumentalities of such offences, and assets of corresponding value?[198]

(m) Transfer criminal proceedings, as appropriate, in terrorism-related cases?[199]

285. Does the State's legislation allow for:

(a) The use of applicable international and regional instruments to which the State is a party as a basis for mutual legal assistance in terrorism cases, and cooperation where possible on the basis of reciprocity or on a case-by-case basis, in the absence of applicable conventions or provisions?[200]

(b) Effective implementation of its respective bilateral and multilateral treaties concerning extradition and mutual legal assistance in criminal matters related to counter-terrorism?[201]

(c) Simplified extradition and mutual legal assistance requests in terrorism-related cases, within the framework of the implementation of existing applicable international legal instruments, while ensuring that relevant legal obligations are upheld and, in particular, the need for due consideration?[202]

(d) The broadest possible international cooperation, including the appointment of liaison officers, police-to-police cooperation, the creation and use, when appropriate, of joint investigation mechanisms, and enhanced coordination of

[196] Counter-Terrorism Committee, "Policy guidance on international cooperation: policy guidance PG.3", June 2010, para. 2; and resolution 2482 (2019), para. 15 (b).

[197] Resolution 1373 (2001), para. 3 (a); Council of Europe Convention on Cybercrime, art. 26; Arab Convention on Combating Information Technology Offences, art. 33; Council Framework Decision 2005/222/JHA, art. 11; and Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, art. 14.

[198] International Convention for the Suppression of the Financing of Terrorism.

[199] Resolution 2322 (2016), para. 9 (b).

[200] Ibid, para. 13 (a).

[201] Ibid, para. 13 (c).

[202] Ibid, para. 13 (d).

cross-border investigations in terrorism cases, and the use of electronic communication and universal templates, in full respect for the fair trial guarantees of the accused?[203]

(e) The transfer of criminal proceedings, as appropriate, through appropriate laws and mechanisms, in terrorism-related cases?[204]

(f) Evidence to be taken by videoconference in the requested State if it is not possible or desirable, for another reason, for the person in question to appear at proceedings in the requested party?

(g) Provisions on temporary transfer of detained persons to the requested State for the purpose of investigation?

(h) Spontaneous transmission of information?

(i) Provision of assistance, both in the absence of, and pursuant to, a treaty arrangement?

(j) Empowering the central authority to enforce conditions and limitations upon request?

(k) Mutual legal assistance in the context of:

(i) Special investigative techniques?

(ii) Provisions on admissibility of evidence gathered in other jurisdictions, when appropriate?

(iii) Access to and collection and disclosure of computer data at the request of a foreign State?[205]

3. Central authority

286. In paragraph 13 (e) of its resolution 2322 (2016), the Council calls on States to designate central authorities or other relevant criminal justice authorities to handle mutual legal assistance and extradition matters and to ensure that such authorities have adequate resources, training and legal authority, in particular for terrorism-related offences.

287. In paragraph 13 (f) of that same resolution, the Council further calls on States to take measures, where appropriate, to update current practices on mutual legal assistance regarding acts of terrorism, including considering, where appropriate, the use of electronic transfer of requests to expedite proceedings between central authorities or, as appropriate, other relevant criminal justice authorities, with full respect for existing treaty obligations.

288. Member States are also called upon to consider submitting to the UNODC repository database contact information and other relevant details concerning their designated authorities.[206]

289. The following issues should be considered:

(a) Has the State designated a central authority or other relevant criminal justice authority to handle mutual legal assistance and extradition matters?[207]

[203] Ibid, para. 15.
[204] Ibid, para. 9 (b).
[205] Resolution 1373 (2001), para. 3 (a); Council of Europe Convention on Cybercrime, arts. 30–34; and Arab Convention on Combating Information Technology Offences, arts. 38–42.
[206] Resolution 2322 (2016), para. 13 (g).
[207] Ibid, para. 13 (e).

(b) Do such authorities have adequate resources, training and legal authority, in particular for terrorism-related offences?[208]

(c) Is the central authority able to use applicable international instruments to which the State is a party as a basis for mutual legal assistance and, as appropriate, for extradition in terrorism cases and, in the absence of applicable conventions or provisions, to cooperate where possible on the basis of reciprocity or on a case-by-case basis?[209]

(d) Has the State put in place appropriate mechanisms that allow for the broadest possible international cooperation, including the appointment of liaison officers, police-to-police cooperation, the creation and use, when appropriate, of joint investigation mechanisms, and enhanced coordination of cross-border investigations in terrorism cases, and the use of electronic communication and universal templates, in full respect for the fair trial guarantees of the accused?[210]

(e) Has the State ensured the use of up-to-date mutual legal assistance practices, including, where appropriate, the use of electronic transfer of requests to expedite proceedings between central authorities or, as appropriate, other relevant criminal justice authorities, with full respect for existing treaty obligations?[211]

(f) Has the State submitted to the UNODC repository database contact information and other relevant details concerning its designated authorities?[212]

(g) Is the central authority able to train officials, judges and prosecutors in drafting and executing mutual legal assistance and extradition requests?

(h) Does the central authority coordinate seizure and confiscation actions with other States?

(i) Has the central authority concluded effective bilateral or multilateral arrangements and channels to cooperate with other authorities (central, judicial, prosecutorial and law enforcement)?

(j) Has the central authority concluded effective bilateral or multilateral arrangements and channels to coordinate cross-border investigations and prosecutions?

(k) Has the central authority concluded bilateral or multilateral arrangements on controlled delivery, covert investigations and joint investigation teams?

(l) Has the central authority established mechanisms for cooperation and consultation before refusal of a mutual legal assistance or extradition request or before postponing execution of such a request?

(m) Does the State participate in regional mutual legal assistance cooperation platforms and has it taken steps to develop or enhance, as appropriate, arrangements for expeditious cross-regional cooperation for terrorism-related offences?[213]

(n) Does the central authority have adequate resources, training and legal authority, in particular for terrorism-related offences?

[208] Ibid, para. 13 (e).
[209] Ibid, para. 13 (a).
[210] Ibid, para. 15; resolution 2482 (2019), para. 15 (b).
[211] Resolution 2322 (2016), para. 13 (f).
[212] Ibid, para. 13 (g); and Counter-Terrorism Committee, “Policy guidance on international cooperation”, para. 2 (k).
[213] Resolution 2322 (2016), para. 13 (h).

(o) Does the central authority have the capacity to serve as a round-the-clock point of contact in the absence of a distinct established round-the-clock focal point?[214]

(p) Is the central authority able to disseminate guidance on national mutual legal assistance and extradition requirements both to domestic practitioners and to foreign authorities?

(q) Is the central authority able to make use of alternatives to mutual legal assistance and extradition (and does it in fact do so)?

(r) Does the central authority have the capacity to take practical measures with a view to facilitating the rapid execution of a request?

(s) Is the central authority able to transfer criminal proceedings?[215]

290. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principles 33–35;

(b) Addendum to the Madrid Guiding Principles, guiding principle 49;

(c) Counter-Terrorism Committee, "Policy guidance on international cooperation: policy guidance PG.3", 14 June 2010, para. 2 (f);

(d) UNODC, *Manual on International Cooperation in Criminal Matters related to Terrorism* (New York, 2009);

(e) UNODC Mutual Legal Assistance Request Writer Tool;

(f) UNODC model laws on international cooperation;

(g) Financial Action Task Force recommendations 36–40;

(h) Sahel Fusion and Liaison Unit;

(i) Council of the European Union resolution 2017/C 18/01 on a model agreement for setting up a joint investigation team;

(j) International Association of Prosecutors Counter-Terrorism Prosecutors Network;

(k) Practical guide to extradition and mutual legal assistance for the States members of the Indian Ocean Commission;

(l) Practical guide on carrying out effective extradition and mutual legal assistance requests in criminal matters for States members of the Sahel Judicial Platform.

O. Effective border security and related issues[216]

291. Effective border security and overall border management is essential in countering terrorism because it constitutes the first line of defence against the cross-border movement of terrorists and illicit goods and cargo.[217] In paragraph 2 (g) of its resolution 1373 (2001), the Council requires States to prevent the movement of

[214] Resolution 1373 (2001), para. 3 (a); Council of Europe Convention on Cybercrime, art. 35; Council Framework Decision 2005/222/JHA, art. 11; and Arab Convention on Combating Information Technology Offences, art. 43.

[215] S/2015/975, annex, para. 40.

[216] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.1, 2, 11 and 23.

[217] S/2016/49, annex, para. 424.

terrorists or terrorist groups by effective border controls and controls on the issuance of identity papers and travel documents. Similarly, in paragraph 2 of its resolution 1624 (2005), the Council calls upon all States to cooperate to strengthen the security of their international borders, including by combating fraudulent documents and enhancing screening measures. Effective border security and management is of particular importance with respect to foreign terrorist fighters, as reflected in paragraphs 2, 8, 9 and 11 of resolution 2178 (2014) and in resolution 2396 (2017). In the preamble to resolution 2322 (2016), the Council reiterates the obligation of States to prevent the movement of terrorists and terrorist groups, in accordance with applicable international law, and underlines the importance of strengthening international cooperation in stemming the flow of foreign terrorist fighters. In para. 15 (a) of its resolution 2482 (2019), the Council calls upon States to strengthen border management to effectively identify and prevent the movement of terrorists, terrorist groups and transnational organized criminals working with them.

292. In order to screen travellers effectively at ports of entry, a combination of several mechanisms needs to be in place, depending on whether the border is an air, maritime or land border. At airports, key mechanisms include advance passenger information, passenger name records, biometric technology and INTERPOL databases.[218] A further element in ensuring effective border control is implementation of the World Customs Organization's SAFE Framework of Standards to Secure and Facilitate Global Trade, which enables States to balance security controls with trade facilitation through risk analysis and targeted inspections.[219]

293. In order to address effectively the cross-border flow of foreign terrorist fighters, appropriate information about the identity of known, suspected or potential fighters upon which border authorities can make informed decisions should be made available in a timely manner to border posts and other relevant agencies, for further action. Information on foreign terrorist fighters may be either specific or general in nature. Specific information includes information obtained from sources such as law enforcement and intelligence agencies and sometimes even the military; advance passenger information; passenger name records; biometrics; national and international watch lists and databases; INTERPOL Notices, including the foreign terrorist fighter criminal analysis file; INTERPOL Diffusions; analytical products; and informants. General information includes the results of trends analysis and risk assessments.

294. Airports continue to be targeted by terrorist groups. The Convention on International Civil Aviation and its annexes provide important standards for ensuring the safety of civil aviation facilities worldwide.[220] In its resolution 2309 (2016), the Council expresses concern that terrorist groups continue to view civil aviation as an attractive target, and identifies a number of steps to be taken by Member States in order to strengthen implementation of the ICAO Standards and Recommended Practices. In its resolution 2396 (2017), the Council urges Member States to implement the Global Aviation Security Plan developed by ICAO, which provides the foundation for ICAO, Member States, the civil aviation industry and other stakeholders to work together with the shared and common goal of enhancing aviation security worldwide and to achieve five key priority outcomes, namely to enhance risk awareness and response, to develop a security culture and human capability, to improve technological resources and innovation, to improve oversight and quality assurance and to increase cooperation and support, and calls for action at the global,

[218] Resolution 2178 (2014), paras. 9 and 13; statement by the President of the Security Council of 29 May 2015 (S/PRST/2015/11); S/2015/975; and S/2016/49, annex, para. 426.

[219] S/2016/49, annex, para. 430.

[220] Ibid.

regional and national levels, as well as by industry and other stakeholders, in raising the level of effective implementation of global aviation security.

295. In its resolution 2396 (2017), and acting under Chapter VII of the Charter of the United Nations, the Council decides that, in furtherance of resolution 2178 (2014) and the ICAO Standards and Recommended Practices, and for the purpose of preventing, detecting and investigating terrorist offences and travel with full respect for human rights and fundamental freedoms, Member States should establish advance passenger information systems and develop the capability to collect, process and analyse passenger name record data.

296. Biometric identification is an effective tool to counter the threat posed by terrorists who attempt to travel internationally and use falsified travel documents. In its resolution 2322 (2016), the Council explicitly calls on States to share information on individual terrorists and foreign terrorist fighters, including biometrics. In its resolution 2396 (2017), the Council decides that Member States should develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters. The Council also encourages Member States to share this data responsibly among relevant States and with INTERPOL and other relevant international bodies. The conducting of risk assessments and the implementing of appropriate targeting measures by law enforcement agencies at international airports and other entry points are essential to the identification, detection and interception of suspected foreign terrorist fighters and other high-risk passengers. As the Committee notes in the Madrid Guiding Principles, an advance passenger information system enables border authorities to determine passenger risk before flights arrive on their territories, before passengers are approved for boarding in order to detect the departure from their territories, or before the attempted entry into or transit through their territories by suspected foreign terrorist fighters. Such measures are highly dependent on the validity of travel data and other information provided to law enforcement agencies by carriers, shippers, freight forwarders and importers. The flow of passenger-related information from carriers and airlines to law enforcement and border control authorities can be divided into two streams, namely, advance passenger information and passenger name records. The introduction of advance passenger information, supplemented by passenger name records, would greatly assist States to detect foreign terrorist fighters attempting to cross their borders.

297. The design and implementation of comprehensive border management strategies continue to be challenging for many States.[221] Porous borders remain a significant concern, as they can allow terrorists to enter a State without passing through official border points and thereby avoid the examination of documents and screening against national and international watch lists. The monitoring of vast open spaces requires significant resources. Geological and climatic conditions in some States further complicate efforts to control entry to and exit from the territory.[222] The lack of necessary infrastructure at border posts limits officials' access to relevant databases and is often compounded by the fact that officials at one border post may be required to monitor extensive areas beyond official crossing points.[223]

298. The efficacy of any border management system will depend on adequate coordination and information-sharing by various government entities, both within States and between States. It is essential that States continue to focus on these operational issues, including the need for information on persons and goods entering and exiting the State to be shared between officials working at border crossing points

[221] S/2016/501, para. 63.
[222] S/2015/683, annex, para. 66; and S/2015/975, annex, paras. 71, 87, 96 and 133.
[223] S/2015/975, annex, paras. 55 and 68.

and those in other parts of the State.[224] The Council reiterates the importance of considering those issues in the preamble to its resolution 2322 (2016).

299. In its resolution 2178 (2014), the Council requires States to take steps to prevent the entry into, or transit through, their territories of any suspected foreign terrorist fighters. In addition to criminalization, some States have imposed administrative measures to that end, including the imposition of travel bans or the withdrawal of travel documents. Such measures must be implemented in a manner consistent with international human rights law and with appropriate due process protections.

300. In its resolution 2341 (2017), the 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. It also recognizes that protection efforts entail multiple streams of efforts, including risk management for protection programmes and activities and supply chain integrity and security. The Council calls upon Member States to enhance their cooperation to protect critical infrastructure, including regional connectivity projects and related cross-border infrastructure, from terrorist attacks, as appropriate, through bilateral and multilateral means in information-sharing, risk assessment and joint law enforcement.

301. In implementing these border control measures, Member States must also comply with international human rights and refugee law (see also chapter III, section D, "Measures with respect to refugees and asylum").[225]

1. Legal framework

302. The following issues should be considered:

(a) Does the State have in place legislation to prevent illegal entry by terrorists?[226]

(b) Does the State have in place legislation to prevent the smuggling of terrorists?[227]

(c) Does the State regulate inter-agency cooperation through official acts or memorandums of understanding in order to provide a clear definition of activities, tasks and responsibilities covering the whole spectrum of border security and management?[228]

(d) Does national legislation clearly regulate the way in which States can collect, use, retain and transfer advance passenger information and passenger name record data in accordance with the ICAO Standards and Recommended Practices, domestic law and international obligations, and with full respect for human rights and fundamental freedoms, including by being consistent with article 17 of the International Covenant on Civil and Political Rights? (For more information on advance passenger information and passenger name records, see also chapter II,

[224] Ibid., annex, paras. 70, 84, 134 and 156 (c); and Global Counterterrorism Forum, The Hague-Marrakech Memorandum on Good Practices for a More Effective Response to the Foreign Terrorist Fighter Phenomenon, good practice 10.

[225] Resolution 1624 (2005), para. 4; and resolution 2178 (2014), para. 5.

[226] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.1.

[227] Ibid., template 2.10.2; and S/2016/49, annex, para. 427.

[228] Global Counterterrorism Forum, "Good practices in the area of border security and management in the context of counterterrorism and stemming the flow of 'foreign terrorist fighters'", good practice 2.

section O, “Effective border security and related issues”, subsection 14, “Effective use of advance passenger information and passenger name records”.)

(e) Does the State have in place appropriate legislation for the establishment and use of watch lists or databases of known and suspected terrorists, including foreign terrorist fighters, and to enable appropriate sharing of such information? (For more information on watch lists and databases, see also chapter II, section O, “Effective border security and related issues”, subsection 15, “Establishing and maintaining integrated counter-terrorism watch lists or databases”.)

(f) Does the State have in place appropriate legislation ensuring the responsible use of biometric data? (For more information on the responsible use of biometric data, see also chapter II, section O, “Effective border security and related issues”, subsection 16, “Biometric identification”.)

2. Strategy and awareness

303. The following issues should be considered:

(a) Does the State have in place a coordinated border management strategy that clearly formulates the goals to be achieved for a period of three to five years?[229]

(b) Has the State established a national action plan in the context of border security and management describing relevant specific activities in the area of counter-terrorism?[230]

(c) Do the competent authorities use decision analysis tools, such as a strength, weakness, opportunity and threat analysis or force field diagram, to facilitate the development of border security and management and the national action plan?

(d) Are all relevant stakeholders that are meant to facilitate, lead and supervise the implementation of the national action plan (neighbouring States’ public administration and internal organizations involved in border security and management, readmission and reintegration, and border traffic at international airports) identified?

(e) Has the State designated an inter-agency working group responsible for the implementation of the national action plan and consisting of relevant ministries and their departments?

(f) Has the State taken measures to raise awareness among border guards of the foreign terrorist fighter phenomenon?[231]

(g) Have border guards received training on the definition of foreign terrorist fighters, with particular reference to the preparatory nature of the conduct criminalized in resolution 2178 (2014)?

(h) Have border guards received training in how to identify foreign terrorist fighters?

(i) Have border guards received training on the specific challenges associated with identifying female foreign terrorist fighters?[232]

(j) Have border guards received training in protecting and promoting the rights of the child when implementing border management strategies, including

[229] Madrid Guiding Principles, guiding principles 20 and 21.

[230] Global Counterterrorism Forum, “Good practices in the area of border security and management”, good practice 13.

[231] S/2015/939, annex I, group II (a); and Madrid Guiding Principles, guiding principle 18.

[232] Madrid Guiding Principles, guiding principle 18 (f); S/2015/975, annex, para. 27; and resolution 2396 (2017).

training in identifying children who may be victims of parental abductions, criminal abductions (kidnappings) or unexplained disappearances, and how to handle such cases appropriately?

(k) Has the State adopted a border community-oriented policing approach?[233]

(l) Are border authorities engaged on the basis of partnership and dialogue with border communities to raise awareness among border communities of the threat posed by terrorism?

(m) Have the border authorities established a dialogue with all elements of border communities (including tribal chiefs, ethnic groups, religious leaders and nomads) and representatives of civil society?

(n) Do the border authorities involve border communities in the development, implementation and evaluation of strategies, action plans, policies and measures related to border security and management?

(o) Are the national border security and management authorities available, visible and accessible for border communities and nomad tribes?

(p) Are the competent authorities able to analyse the evolution of threats likely to affect the security of external borders and set the priorities for action accordingly?

(q) Are the competent authorities able to develop strategic plans for the implementation of operational and tactical plans?

(r) Are the competent authorities able to anticipate needs relating to human resources and equipment in order to ensure security at external borders, in accordance with the level of risk in different areas?

(s) Do the State's Government and border services adopt a focused approach to tackling corruption in certain key areas, such as identity verification, travel documentation, detection of criminal offences and monitoring of cross-border commerce?[234]

(t) Has the State's Government considered developing national anti-corruption strategies and action plans to cultivate an anti-corruption culture in border security and management-related issues?

3. Documentation

304. The following issues should be considered:

(a) Has the State developed a set of objective criteria for the placement of an individual on watch lists and no-fly lists? (For more information on watch lists and databases, see also chapter II, section O, "Effective border security and related issues", subsection 15, "Establishing and maintaining integrated counter-terrorism watch lists or databases".)[235] Has the State developed processes to ensure that the personal data contained in such lists is complete, accurate and up to date?[236]

---

[233] Global Counterterrorism Forum, "Good practices in the area of border security and management", good practice 5.

[234] Global Counterterrorism Forum, "Good practices in the area of border security and management", good practice 15.

[235] S/PRST/2015/11; and Madrid Guiding Principles, guiding principles 15 and 37.

[236] Madrid Guiding Principles, guiding principles 15 and 37; and Counter-Terrorism Committee Executive Directorate, "Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions", 2017, p. 64.

(b) Does the State have the necessary safeguards in place to ensure that information contained in watch lists and no-fly lists is not misused in a manner that threatens human rights and is maintained with full respect for the right to privacy?[237]

(c) Does the State have the capacity to prevent and detect fraudulent use of identity and travel documents?[238]

(d) Does the State issue secure ICAO-compliant machine readable travel documents?[239]

(e) Does the State issue secure "breeder" primary documents?[240]

(f) Does the State have the capacity to confirm the authenticity of "breeder" primary documents before issuing travel documents (i.e., through verification with civil registries, electronically, or by other means)?[241]

(g) Does the State incorporate into its travel documents unique and distinctive designs and materials that are difficult to counterfeit?[242]

(h) Does the State regularly include stolen and lost travel documents and passports in national watch lists and alerts?[243]

(i) Does the State regularly communicate relevant data on stolen and lost passports to INTERPOL?[244]

(j) Does the State revoke the travel documents of suspected foreign terrorist fighters? If so:

(i) What is the duration of such measures?

(ii) Does the State record the revocation in a national database?

(iii) Does the State inform international partners of the revocation (e.g., by recording it in the INTERPOL Stolen and Lost Travel Document Database)?

(iv) What procedures are in place to enable affected individuals to challenge those measures?

4. National practices to prevent terrorist movements, including movements of foreign terrorist fighters

305. The following issues should be considered:

(a) Does the State have in place measures to prevent foreign terrorist fighters from crossing its national borders (e.g., travel bans or withdrawal of travel documents)?

(b) Does the State know the prerequisites for those measures?

(c) Does the State have procedures in place to safeguard due process and the right to freedom of movement?

---

[237] S/PRST/2015/11; and Madrid Guiding Principles, guiding principles 15 and 37.
[238] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.7; and resolution 2178 (2014), para. 2.
[239] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.12.
[240] Ibid., template 2.10.13 (A).
[241] Ibid., template 2.10.13 (B).
[242] Ibid., template 2.10.13 (C).
[243] Ibid., template 2.10.14.
[244] Ibid., template 2.10.15.

(d) Does the State have in place a procedure to ban potential or suspected foreign terrorist fighters from travelling to conflict zones?

(e) Does the State have in place a procedure to apply a court decision to ban potential or suspected foreign terrorist fighters from travelling, with confiscation of their passport, including when a passport is not needed to travel to some destinations? (See also chapter II, section O, "Effective border security and related issues", subsection 3, "Documentation".)

5. Screening prior to arrival in the destination State

306. The following issues should be considered:

(a) Does the State have the intelligence and analytical capacity to detect potential terrorists?[245]

(b) Does the State have in place procedures to prevent suspected foreign terrorist fighters from transiting through airports within its territory?[246]

(c) Has the State established a dedicated analytical team for the timely review of information relating to existing or potential foreign terrorist fighters?[247]

(d) Do the State's consulates and embassies abroad check visa applicants' details against national and international watch lists?

(e) Does the State have in place measures for the advance screening of persons travelling from States benefiting from visa-free or visa-upon-arrival arrangements?[248]

(f) Does the State have personnel and facilities for the screening of women and girls in contexts where separate facilities and personnel may be necessary?

(g) Does the State have access to pre-arrival traveller information (through advance passenger information systems) for risk assessment purposes?

(h) Does the State receive passenger name records for passengers travelling by air? (For more information on advance passenger information and passenger name records, see also chapter II, section O, "Effective border security and related issues", subsection 14, "Effective use of advance passenger information and passenger name records".)

307. For issues relating to information management consistent with international human rights law, see also chapter IV, section B, "Measures with respect to entry and asylum screening for people who may have been guilty of incitement to commit a terrorist act".

6. Screening upon arrival at the border

308. The following issues should be considered:

(a) Has the State considered establishing joint border crossing points with the competent authorities of partner States to address the crossing of external borders?

(b) Does the State consistently and effectively screen persons for potential links to terrorism prior to their entry into its territory?[249]

---

[245] Ibid., template 2.10.7; and Madrid Guiding Principles, guiding principles 15–19.

[246] Implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters (S/2015/338, annex), para. 42.

[247] Madrid Guiding Principles, guiding principle 16.

[248] S/2015/338, annex, para. 43; and Madrid Guiding Principles, guiding principles 15–19.

[249] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.3; and resolution 2178 (2014), para. 2.

(c) Does the State conduct threat assessments with respect to passengers benefiting from visa-free or visa-upon-arrival arrangements?[250]

7. Access to information by border guards

309. The following issues should be considered:

(a) Is the State's immigration screening process connected at the front line to national watch lists or databases and alerts?

(b) Is the State's immigration screening process connected at the front line to the INTERPOL I-24/7 system, the Stolen and Lost Travel Documents Database and Red Notices for suspected criminals and wanted persons, as well as the ISIL (Da'esh) and Al-Qaida sanctions list?[251]

(c) Does the State use the Mobile INTERPOL Network Database and the Fixed INTERPOL Network Database?[252]

(d) Does the State authenticate electronic machine readable travel documents using the ICAO Public Key Directory?

(e) Does the State have access to the UNODC goCASE system?[253]

(f) Has the State developed and implemented information exchange programmes and mechanisms related to border security and management, both at border crossing points and along borders?

(g) Has the State considered adopting a broader format to exchange relevant information that involves the information systems of the Ministry of the Interior and the Ministry of Finance, or their equivalents, and their various agencies (i.e., criminal police, organized crime units, intelligence services, immigration services and visa authorities)?

(h) Has the State considered downgrading for official use intelligence threat data on foreign terrorist fighters and individual terrorists in order to provide such information to front-line screeners, such as immigration, customs and border security agencies, where appropriate?[254]

(i) Has the State put in place mechanisms to ensure the efficiency and reliability of the four categories of information exchange ("on request", "ad hoc", "periodic" and "continuous") through joint databases?

(j) Does the State assign experts to conduct effective risk analysis assessments to address and minimize gaps between risks and capabilities? If so:

(i) Is the joint risk analysis process systematic and continuous, with agreed upon and clearly defined content, matrix structure and measures to process relevant information?

(ii) Do customs officers perform checks and surveillance at external borders in accordance with national legislation and international law, including bilateral and multilateral treaties?

---

[250] S/2015/338, annex, para. 43.

[251] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.5.

[252] Ibid., template 2.10.6; and Global Counterterrorism Forum, The Hague-Marrakech Memorandum on Good Practices for a More Effective Response to the Foreign Terrorist Fighter Phenomenon, good practice 13.

[253] Global Counterterrorism Forum, "Good practices in the area of border security and management", good practice 3.

[254] Resolution 2322 (2016), para. 5.

(iii) Are relevant data categorized by border type (land, air and sea)?

(iv) Are all collected data analysed on a weekly, monthly, quarterly and annual basis?

(k) Does the risk analysis include development and understanding of common key indicators, such as:

(i) Detection of illegal border crossings across green and blue borders or bypassing border crossing points?

(ii) Refusal of entry or exit for travellers?

(iii) Detection of illegal stays, both inland and at the exit border?

(iv) Detection of human traffickers and people smugglers?

(v) Detection of forged travel documents and visas?

(vi) Administrative decisions for return, readmission or expulsion?

(vii) Data on asylum applications?

(l) Does the State involve a broad range of government agencies and ministries in the joint risk analysis?

(m) Is the State able to identify the lead border security and management agency in the risk assessment for a range of threat scenarios?

(n) Do border guard units receive updated information on new methods used by foreign terrorist fighters to cross borders, including broken travel patterns?[255]

(o) Have the competent authorities put in place hotline numbers?

(p) Is the hotline infrastructure able to triage incoming calls so that information is immediately actionable, treated with the highest priority and directed to the correct operational agency almost immediately?

(q) Do border guards systematically add information on foreign terrorist fighters to national and international watch lists?[256]

(r) Are the systems operating biometric data interoperable with border biometric applications, including with biometric databases provided by INTERPOL, permitted by national law?

(s) What measures has the State taken to maximize its use of the INTERPOL biometric databases, including facial recognition, fingerprints and DNA profiles? (For more information on biometric identification, see also chapter II, section O, “Effective border security and related issues”, subsection 16, “Biometric identification”.)

310. For issues relating to the use of the Customs Enforcement Network secure platform and the Regional Intelligence Liaison Office network of the World Customs Organization, see also chapter II, section D, “Taking the steps necessary to prevent the commission of terrorist acts, through the provision of early warning”, subsection 2, “Early warning”.

[255] S/2015/338, annex, paras. 40 and 41.

[256] S/PRST/2015/11; Madrid Guiding Principles, guiding principle 17; and Global Counterterrorism Forum, The Hague-Marrakech Memorandum on Good Practices for a More Effective Response to the Foreign Terrorist Fighter Phenomenon, good practice 14.

8. Screening after arrival in the State

311. The following issues should be considered:

(a) Does the State systematically seek to identify individuals who have no legal basis for remaining in the State?[257]

(b) Does the State have effective in-country screening measures (e.g., prior to adjustment of legal status, issuance of work permit, granting of permanent residence or citizenship) to prevent the extension of residency to terrorists?[258]

9. Intra-agency cooperation

312. The following issues should be considered:

(a) Are formal written arrangements developed, inter alia, in the areas of standard operational procedures, reporting and communication, analysis methods, and coordination of workflow mechanisms?[259]

(b) Are informal arrangements developed for unit-to-unit or person-to-person exchange of information, consultations, opinions or advice during daily operations?

10. Coordination with other State agencies

313. The following issues should be considered:

(a) Do border guards share with other State agencies information obtained on individual cases or on evolving foreign terrorist fighter profiles?

(b) Do relevant State agencies (e.g., customs, financial intelligence unit, police) proactively share information with border guards regarding suspected foreign terrorist fighters (i.e., before such persons attempt to exit the territory)?

(c) Has the State considered enhancing inter-agency cooperation through common communication platforms, such as information technology systems, to facilitate the sharing of information and intelligence?

(d) Are all the ministries involved in the area of border security and management (e.g., ministries of foreign affairs, defence, health) included in inter-agency coordination structures?

(e) Are there procedures in place for border guards to provide feedback on the validity and utility of information on foreign terrorist fighters received from other State agencies, as well as information on results achieved?

(f) Have the national authorities considered aligning border crossing facilities and procedures with those of neighbouring or contracting authorities (i.e., joint border crossing points or “one-stop-shop” border crossing points)?

(g) Does the State record and store (in an automated system) the entry and exit of persons crossing its borders?[260]

---

[257] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.9.

[258] Ibid., template 2.10.10.

[259] Global Counterterrorism Forum, “Good practices in the area of border security and management”, good practice 1.

[260] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.8.

(h) Is there robust collaboration between non-security services (border guards, border police) and customs agencies, as well as with security services (police and defence forces)?[261]

(i) Has the State concluded bilateral or multilateral agreements to establish border cooperation centres as joint cooperation centres for border law enforcement agencies?

(j) When border guards identify a suspected foreign terrorist fighter, are there standard procedures in place for the referral of such cases to law enforcement bodies?

11. Coordination with regional and international partners

314. The following issues should be considered:

(a) Does the State have in place measures to cooperate with other States to, inter alia, strengthen the security of their international borders, including by combating fraudulent travel documents and by enhancing terrorist screening and passenger security procedures?[262]

(b) In the absence of an agreement, is the State involved in a procedure to resolve issues of delimitation and demarcation of borders on a bilateral (or multilateral, where applicable) governmental basis?[263]

(c) Have neighbouring States considered establishing inter-agency task forces or fusion centres to handle intergovernmental and interdepartmental efforts to strengthen border security and management?

(d) Does the State conduct joint and coordinated cross-border patrols, as well as joint multi-agency and interdisciplinary operation exercises?

(e) Has the State concluded bilateral or multilateral agreements to enable cross-border operational engagement through joint operations?[264]

(f) If so, do such joint operations involve the patrolling and surveillance of borders through joint mobile units?

(g) If so, are there agreements that address central points, including:

(i) The permissible distance into the neighbouring State under which cross-border operational engagement can take place?

(ii) How a State may seek the transfer of an apprehended suspect from the other State?

(iii) Information exchange in relation to the progress of the investigation and cross-border operational activity?

(h) Has the State appointed and assigned border liaison officers in order to build external relations through face-to-face coordination and knowledge exchange?

(i) Does the State consult regional and international sources of information on foreign terrorist fighters?[265]

---

[261] Global Counterterrorism Forum, “Good practices in the area of border security and management”, good practice 2.

[262] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.16; resolution 2178 (2014), para. 3; and S/2015/975, annex, para. 71.

[263] Global Counterterrorism Forum, “Good practices in the area of border security and management”, good practice 3.

[264] Ibid., good practice 11; and Madrid Guiding Principles, guiding principles 20 and 21.

[265] Madrid Guiding Principles, guiding principle 15 (a).

(j) Has the State undertaken, with the assistance of relevant international organizations and other experts, specific measures to improve understanding of the use of broken travel patterns by foreign terrorist fighters?[266]

(k) Has the State taken measures to share information and experiences on foreign terrorist fighters with neighbouring States?[267]

(l) Is the State involved in the INTERPOL project on foreign terrorist fighters?[268]

(m) Does the State share biometric data with international partners in compliance with international human rights law? (For more information on biometric identification, see also chapter II, section O, "Effective border security and related issues", subsection 16, "Biometric identification".)

12. Movement of goods

315. The following issues should be considered:

(a) Has the State developed integrated procedures for the processing of goods at points of entry, including operations such as goods classification, carrier and goods inspection, revenue collection and transaction verification?[269]

(b) Does the State implement the "single window" and "one-stop-shop" systems?

(c) Does the State receive data (electronic transmission) regarding cargo and container shipments prior to their arrival?[270]

(d) Does the State conduct risk assessments regarding cargo and containers?[271]

(e) Does the State have the capacity (technology, equipment and trained officers) to conduct non-intrusive inspections of cargo entering, exiting, transiting or being trans-shipped through its territory?[272]

(f) Does the State implement customs-to-customs cooperation that includes conducting requested inspections?[273]

(g) Does the State have in place customs-to-business partnerships to implement cargo security standards, including an authorized economic operator programme?[274]

13. Civil aviation security and facilitation

316. In its resolutions 1373 (2001), 2178 (2014) and 2396 (2017), the Council states that all Member States shall prevent the movement of terrorists or terrorist groups through effective border controls and controls on the issuance of identity papers and

[266] Resolution 2178 (2014), para. 11; and Madrid Guiding Principles, guiding principle 16 (c).
[267] Global Counterterrorism Forum, The Hague-Marrakech Memorandum on Good Practices for a More Effective Response to the Foreign Terrorist Fighter Phenomenon, good practice 10.
[268] S/2015/975, annex, paras. 85, 97 and 156 (b); and Global Counterterrorism Forum, The Hague-Marrakech Memorandum on Good Practices for a More Effective Response to the Foreign Terrorist Fighter Phenomenon, good practice 10.
[269] Global Counterterrorism Forum, "Good practices in the area of border security and management", good practice 13.
[270] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.17 (A).
[271] Ibid., template 2.10.17 (B).
[272] Ibid., template 2.10.17 (C).
[273] Ibid., template 2.10.17 (D).
[274] Ibid., template 2.10.17 (E).

travel documents and through measures to prevent counterfeiting, forgery or fraudulent use of identity papers and travel documents. All such measures must be undertaken in accordance with domestic law and international obligations, with full respect for human rights and fundamental freedoms.

317. Appropriate information concerning the identity of existing, suspected or potential foreign terrorist fighters, without resorting to profiling based on any discriminatory grounds prohibited by international law, upon which border authorities can make informed decisions, should be made available in a timely manner to ensure that foreign terrorist fighters are detected during routine border, immigration and police checks.

318. Information on foreign terrorist fighters should be specific and could be supplemented by general information. Specific information includes information obtained from sources such as law enforcement and intelligence agencies and the military; advance passenger information; passenger name records; biometrics; national and international watch lists; INTERPOL databases (including both the foreign terrorist fighter and the stolen and lost travel documents databases) and the system of international notices and diffusions; analytical products; and informants. General information includes the results of trends analyses and risk assessments.

319. In order to maximize opportunities for the detection of foreign terrorist fighters and the prevention of their onward travel, information on foreign terrorist fighters should routinely be compared against information generated during all individual travel, including advance passenger information, border crossing information, biometrics, passenger name records and visa applications, and appropriately shared with all States concerned.

320. The following issues should be considered:

(a) Has the State adopted a regulatory framework and a national civil aviation security oversight system (comprehensive, flexible and effective national aviation security legislation, regulations, programmes, preventive security measures and procedures)?

(b) Has the State adopted the relevant programmes, including:

(i) A national civil aviation security programme?

(ii) A national civil aviation security quality control programme (authority, responsibility, and a mechanism for conducting audits, tests, surveys and inspections of all aviation security measures implemented in the aviation security system by all agencies, authorities, aircraft operators and others concerned)?

(iii) A national civil aviation security training programme (comprehensive aviation security training programme for the effective implementation of preventive measures identified in the national civil aviation security programme) and a system for the training, certification and testing of security personnel in order to achieve and maintain an acceptable level of effectiveness and efficiency?

(iv) A national contingency plan?

(c) Has the State adopted national aviation security requirements?

(d) Has the State designated an appropriate government authority for the implementation and maintenance of the national civil aviation security programme? [275]

[275] Ibid., template 2.10.18 (A).

(e) Has the State made available aviation security resources at the national level, in order to ensure that an effective and sustainable aviation security system is in place?

(f) Has the State adopted written policies requiring cooperation with other States on various aspects of aviation security?

(g) Has the State established policies for international cooperation on aviation security on a bilateral and/or multilateral basis?[276]

(h) Has the State implemented such policies?[277]

(i) Has the State implemented an oversight mechanism in order to determine compliance with annex 17 to the Convention on International Civil Aviation at both the national and airport levels? Critical elements of a State's security oversight system shall include:

(i) Aviation security legislation;

(ii) Aviation security programmes and regulations;

(iii) Appropriate State authority for aviation security and its responsibilities;

(iv) Personnel qualifications and training;

(v) Provision of technical guidance, tools and security critical information (see also the reference to appendix 27 of the ICAO *Aviation Security Manual* in chapter II, section C, "Eliminating the supply of weapons to terrorists");

(vi) Certification and approval obligations;

(vii) Quality control obligations;

(viii) Resolution of security concerns.

(j) Does the State conduct regular threat assessments, audits, tests and inspections to verify compliance and rectify deficiencies?[278]

(k) Does the State have a programme to assist other States in aviation security capacity development, including training and other necessary resources, technical assistance, technology transfers and programmes?

(l) Has the State made efforts to implement the Global Aviation Security Plan and to fulfil the specific measures and tasks assigned to States in appendix A to the Plan, the Global Aviation Security Plan Road Map?

(m) Does the State have the capacity to enhance risk awareness and response and ensure wider understanding of the threats and risks facing civil aviation?

14. Effective use of advance passenger information and passenger name records

321. The following issues should be considered:

(a) Has the State established an advance passenger information system, for the purpose of preventing, detecting and investigating terrorist offences and travel in full respect for human rights and fundamental freedoms?

(b) Has the State required airlines operating in its territory to provide advance passenger information to the appropriate national authorities?

[276] Resolution 2309 (2016), para. 6 (f).
[277] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.18 (A).
[278] Ibid., 2.10.18 (B).

(c) Are adequate resources available to implement effective advance passenger information and passenger name record systems?

(d) Are air carriers obligated to transfer advance passenger information and passenger name record data to the relevant national authorities (single window and passenger information units)?

(e) Has the State established or designated specific entities responsible for the collection, storage, processing and analysis of passenger name records and advance passenger information data received from air carriers (e.g., through the establishment of passenger information units and capacity-building efforts)?

(f) Do the passenger information units compare passenger name records and advance passenger information data against relevant law enforcement databases and process them against pre-determined criteria to identify persons who may be involved in a terrorist offence, without resorting to profiling based on any discriminatory grounds prohibited by international law? Do the passenger information units reply, on a case-by-case basis, to duly reasoned requests for passenger name records and advance passenger information data originating from the competent authorities?

(g) Has the State designated and assigned a data protection officer to the passenger information unit who is responsible for monitoring the processing of passenger name record data and for implementing relevant safeguards?

(h) Is appropriate advance passenger information and passenger name record data shared with relevant or concerned Member States to detect foreign terrorist fighters returning to their countries of origin or nationality or travelling or relocating to a third country, with particular regard for all individuals designated by the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities, with full respect for human rights and fundamental freedoms?

(i) Does the State allow for such data to be compared against, for instance, INTERPOL databases and United Nations sanctions lists?

(j) Do passenger name record data-processing and retention frameworks incorporate oversight and privacy protections? Are precautions taken against the misuse or abuse of the data by State authorities?

(k) Does the State ensure respect for the data subjects' right to freedom from arbitrary or unlawful interference with their privacy under international law, as well as for relevant protections under national law, which may include access, rectification, restrictions on use and judicial redress?

15. Establishing and maintaining integrated counter-terrorism watch lists or databases

322. The following issues should be considered:

(a) Has the State developed a watch list or database of known and suspected terrorists, including foreign terrorist fighters, for use by law enforcement, border security, customs, the military and intelligence agencies to screen travellers and conduct risk assessments and investigations, in compliance with domestic and international law, including human rights law?

(b) Has the State ensured effective oversight of the entire watch list or database, paying particular attention to data management functions and the purposes for which the data are to be used and the need to avoid any unauthorized extension of scope or access?

(c) Has the State verified that clear and appropriate criteria, including with respect to the definitions of terrorist acts, are consistent with Council resolutions and the State's obligations under international counter-terrorism conventions, and are developed and relied upon for the inclusion of persons' names in watch lists and databases?

(d) Has the State implemented a regulatory framework for the enrolment, use, review, retention and deletion of data from the watch list or database? What measures has the State taken to ensure that the communications network is secured and that appropriate security levels are in place to protect the operational environment, including the data, hardware, software and communications network?

(e) Has the State developed and implemented specific frameworks and safeguards to protect and promote the rights of the child in situations where children may be placed on watch lists or databases, including in situations where children are placed on databases for child protection purposes?

(f) What measures has the State taken to ensure that the watch list or database includes input from authorized relevant law enforcement agencies and is thus sufficiently comprehensive?

(g) What measures has the State taken to ensure that the watch list or database is accessible to the relevant law enforcement agencies and border authorities?

(h) Has the State put in place appropriate safeguards and procedures to ensure that the actions and responses of all relevant law enforcement agencies and border authorities, based on a match received from a watch list or database, are in compliance with domestic and international law, including human rights law?

16. Biometric identification

323. The following issues should be considered:

(a) Do the competent authorities compare the biometrics of individuals entering, departing or seeking residence in their country against other national and international biometric databases, including those of known and suspected foreign terrorist fighters?

(b) What measures has the State taken to develop or increase its use of biometric systems in a responsible and proper manner to authenticate the identity of individuals and prevent them from presenting false particulars or attempting to impersonate other people?[279]

(c) Are biometric databases and data-sharing protocols maintained effectively?

(d) Has the State adopted a clear human rights-based framework for the use of biometric technology, which includes the use of procedural safeguards and effective oversight of its application, including by establishing or expanding the remit of existing appropriate oversight bodies to supervise the implementation of relevant legislation and the provision of effective remedies in case of violations in that regard, or alternatively, supplemented by a review process that informs all national policymaking and decision-making regarding the use of biometrics for counter-terrorism purposes?

(e) Has the State put in place specific, appropriate legal frameworks and safeguards to protect and promote the rights of the child in situations where children's

[279] Counter-Terrorism Committee Executive Directorate, "Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions", 2017, p. 64.

biometric data are collected, including when the data are collected for child protection purposes?

(f) Does the State conduct regular risk assessments of the end-to-end processes of its biometric applications in order to mitigate current or emerging threats, such as identity theft, deletion and replacement of data, and deliberate damage?

(g) What measures has the State taken to ensure that actions taken by the authorities as a result of biometric matches are considered in the context of international law, including international human rights obligations, and the need for a fully informed, lawful response?

(h) Do the systems operating biometric data and the legal frameworks associated with their use allow for interoperability between other national and international biometric databases, including those of INTERPOL, and maximize the use of the INTERPOL biometric databases (facial recognition, fingerprints and DNA)?

17. Airport security

324. The following issues should be considered:

(a) Does the State ensure that an airport security programme is developed and implemented at every airport serving civil aviation?[280]

(b) Are the measures in place at airports in the State's jurisdiction risk-based? Are those measures regularly and thoroughly assessed to reflect the ever-evolving threat picture and in accordance with the ICAO Standards and Recommended Practices?

(c) Does the State promote an effective aviation security culture? If so, how?

(d) Does the State ensure that persons implementing security controls are subject to background checks and obtain the necessary training and certification?[281]

(e) Do the security measures in place take into account the potential role of those with privileged access to areas, knowledge or information that may assist terrorists in planning or conducting attacks?[282]

(f) Does the State have in place an identification system for persons and vehicles prior to granting access to airside and restricted areas at civil aviation airports, in order to prevent unauthorized entry? (See also chapter II, section O, "Effective border security and related issues", subsection 3, "Documentation".)[283]

(g) Does the State regularly verify the security of perimeter fences around such restricted areas?

(h) Does the State screen the cabin and hold baggage of originating and transfer passengers prior to boarding or loading of the aircraft and ensure that each piece of hold baggage is individually identified as accompanied or unaccompanied before acceptance for carriage?[284]

---

[280] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.18 (C).

[281] Ibid., template 2.10.18 (D).

[282] Resolution 2309 (2016), para. 6 (c).

[283] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.18 (E).

[284] Ibid., template 2.10.19.

(i) Does the State screen originating and transfer passengers prior to boarding or loading of the aircraft?

(j) Has the State taken steps to fully utilize new technologies and innovative techniques to detect explosives and other threats to civil aviation?[285]

(k) Does the State have measures in place for aircraft and in-flight security?

(l) Does the State have measures in place for cargo, catering and mail security?

(m) Does the State have contingency arrangements in place for responding to acts of unlawful interference?

18. Maritime security

325. The following issues should be considered:

(a) How do State bodies involved in maritime security (e.g., coastguard, port security, customs, immigration and maritime police) coordinate and cooperate among themselves and with other border management agencies?[286]

(b) Has the State designated a national authority responsible for ship security?[287]

(c) Is there a national legislative basis for implementation of the IMO International Ship and Port Facility Security Code, including legislative authority to promulgate regulations and take all other steps necessary (such as inspection and enforcement) to give full and complete effect to the security directives of the State?

(d) Has the State designated a national authority responsible for port facility security?[288]

(e) Are all the port facilities within the State's territory (and ships entitled to fly the flag of the State and to which the International Ship and Port Facility Security Code applies) in full compliance with the relevant provisions of chapter XI-2 of the International Convention for the Safety of Life at Sea and the International Ship and Port Facility Security Code?

(f) Has the State designated recipients of ship-to-shore security alerts?[289]

(g) Has the State established a recognized security organization?[290]

(h) Has the State designated recipients of maritime security-related communications from other contracting Governments?[291]

(i) Has the State designated recipients of requests for advice or assistance to ships and an agency to which ships can report concerns?[292]

(j) Does the State conduct regular threat assessments, audits, tests and inspections to verify compliance and rectify deficiencies, including updating of security plans?[293]

---

[285] Resolution 2309 (2016), para. 6 (e).
[286] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 2.10.23.
[287] Ibid., template 2.10.20 (A).
[288] Ibid., template 2.10.20 (B).
[289] Ibid., template 2.10.20 (C).
[290] Ibid., template 2.10.20 (D).
[291] Ibid., template 2.10.20 (E).
[292] Ibid., template 2.10.20 (F).
[293] Ibid., template 2.10.20 (G).

(k) Does the State implement a seaport security programme at every seaport used for international trade?[294]

(l) Does the State ensure that persons implementing security controls are subject to background checks and obtain the necessary training and certification?[295]

(m) Does the State have a system in place for checking persons and vehicles before granting them access to seaports, in order to prevent unauthorized entry?[296]

(n) Has the State set up a port security committee at all relevant seaports?[297]

(o) Does the State have procedures in place to register and issue seafarers' manifests and identity documents?[298]

(p) Has the State established the necessary procedures to:

(i) Set applicable security levels (including issuance of appropriate instructions to ship and port facilities that may be affected)?

(ii) Ensure that ship and port facility assessments are conducted, reviewed and approved in accordance with the relevant provisions of the International Ship and Port Facility Security Code?

(iii) Determine which port facilities are required to designate a port facility security officer?

(iv) Determine when a declaration of security is required?

(v) Ensure that ship and port facility security plans are developed, reviewed, approved and implemented in accordance with the relevant provisions of the International Ship and Port Facility Security Code?

(vi) Test the effectiveness of approved ship and port facility security plans?

(vii) Issue and renew International Ship Security Certificates?

(viii) Exercise ship control and compliance measures?

(ix) Receive ship security alerts and subsequent notifications?

(q) Has the State delegated any of its security-related duties under chapter XI-2 of the International Convention for the Safety of Life at Sea and under the International Ship and Port Facility Security Code to a recognized security organization? If so, does the State conduct oversight of delegated tasks and duties? Has the State communicated all relevant information to IMO, as required by regulation XI-2/13 of the International Convention for the Safety of Life at Sea, for the information of companies and ships? Is the information up-to-date and reviewed periodically?

(r) Does the State ensure that port facility security officers and appropriate port facility security personnel have knowledge and have received training, taking into account the guidance set forth in part B of the International Ship and Port Facility Security Code?

(s) Has the State implemented any security measures in addition to those required by chapter XI-2 of the International Convention for the Safety of Life at Sea

[294] Ibid., template 2.10.20 (H).
[295] Ibid., template 2.10.20 (I).
[296] Ibid., template 2.10.20 (J).
[297] Ibid., template 2.10.21.
[298] Ibid., template 2.10.22.

and part A of the International Ship and Port Facility Security Code (e.g., establishment of port or national security committees)?

19. Protecting critical infrastructure, vulnerable or “soft” targets and tourism sites

326. In its resolution 2341 (2017), the Council calls upon States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, including by assessing and raising awareness of the relevant risks; taking preparedness measures, including implementing effective responses to such attacks and promoting better interoperability in security and consequence management; and facilitating effective interaction among all stakeholders involved.

327. In the preamble to and paragraphs 27 and 28 of resolution 2396 (2017), the Council stresses the need for Member 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, and calls on Member States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, to share information and experiences in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks against soft targets.

328. Critical infrastructure and soft targets are especially vulnerable and appealing targets for terrorists. Critical infrastructure vulnerabilities are increased due to the interconnectivity, interlinkage and interdependence of critical infrastructure for States. The appeal of soft targets for terrorists derives not only from their easy access, openness and lower security protection, but also from the possibility to cause massive destruction, high rates of civilian casualties, widespread publicity and fear.

329. Member States bear the primary responsibility for protecting critical infrastructure and soft targets. Each State defines what constitutes critical infrastructure and soft targets in its specific national context. However, in order to maximize the potential to protect such targets, cooperation between States and the private companies that typically own, operate and manage critical infrastructure and soft targets should be increased and strengthened to address security needs, reduce vulnerabilities and share information on threats, vulnerabilities and measures to mitigate the risk. Joint training, communication networks and early-warning mechanisms should be utilized and improved. Member States should cooperate at all levels of government, including local, and engage with communities and civil society.

330. The following issues should be considered:

(a) Has the State defined what constitutes critical infrastructure and soft targets in its national context?

(b) Has the State developed a policy and/or strategy for the protection of critical infrastructure and soft targets?

(c) Has the State developed action plans for reducing the risk of terrorist attacks on critical infrastructure and soft targets? Does the action plan include measures that cover prevention, preparedness, response to, recovery from and investigation of an attack?

(d) Does the State ensure the coherence of its efforts to protect critical infrastructure and soft targets, including with regard to risk management for protection programmes and activities?

(e) Has the State developed a contingency plan that is regularly updated to keep pace with actual threats?

(f) What is the State doing in terms of assessing and raising awareness of the relevant risks and taking preparedness measures, including effective responses to attacks on critical infrastructure or soft targets, in the domain of civil aviation and at maritime and land borders?[299]

(g) Does the State address supply chain integrity and security?

(h) Is there any form of cooperation to protect critical infrastructure, including regional connectivity projects and related cross-border infrastructure?[300]

(i) Is there a dedicated network for cooperation between, on the one hand, relevant public authorities, including at the local level, and, on the other, the private sector, civil society and border communities?

(j) Is consideration given to bilateral and multilateral means of information-sharing, risk assessment and joint law enforcement?

(k) Has the State established public-private partnerships, including for information-sharing purposes, relating to the protection of critical infrastructure and soft targets?

(l) Does the State conduct regular human rights assessments of measures taken to tackle the terrorist threat to critical infrastructure and soft targets and ensure that such measures are evidence-based and therefore efficient?

(a) Movement of persons

331. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principles 15–21;

(b) Addendum to the Madrid Guiding Principles, guiding principles 36–38;

(c) UNHCR, “Addressing security concerns without undermining refugee protection”, Rev.2, 17 December 2015;

(d) UNHCR, *Refugee Protection and Mixed Migration: The 10-Point Plan in Action* (Geneva, 2016);

(e) UNODC, *Basic Training Manual on Investigating and Prosecuting the Smuggling of Migrants* (Vienna, 2010);

(f) International Covenant on Civil and Political Rights;

(g) Human Rights Committee, general comment No. 16 (1988) on the right to privacy (article 17 of the International Covenant on Civil and Political Rights);

(h) Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment;

(i) United Nations Convention against Transnational Organized Crime;

(j) Convention relating to the Status of Refugees and the Protocol thereto;

(k) Convention on the Reduction of Statelessness;

(l) OHCHR, *Recommended Principles and Guidelines on Human Rights at International Borders* (Geneva, 2014);

[299] Resolution 2341 (2017), para. 2.
[300] Ibid, para. 8.

(m) ICAO, *Guidelines on Passenger Name Record (PNR) Data* (Doc. 9944) (Montreal, 2010);

(n) ICAO, *Machine Readable Travel Documents* (Doc. 9303) (Montreal, 2010);

(o) ICAO, *Annex 9 to the Convention on International Civil Aviation: Facilitation* (Montreal, 2017), chapter 3, "Entry and departure of persons and their baggage";

(p) ICAO, *Annex 9 to the Convention on International Civil Aviation: Facilitation* (Montreal, 2017), chapter 5, "Inadmissible persons and deportees";

(q) Reis Oliveira, C., M. Abranches and C. Healy, *Handbook on How to Implement a One-Stop Shop for Immigration* (Lisbon, 2009);

(r) IOM, *Passport Examination Procedure Manual* (Geneva, 2017);

(s) IOM, "IOM and training for border and migration management officials", 2015;

(t) Counter-Terrorism Implementation Task Force, *Basic Human Rights Reference Guide: The Stopping and Searching of Persons* (New York, 2010);

(u) Counter-Terrorism Implementation Task Force, *Basic Human Rights Reference Guide: Security Infrastructure* (New York, 2014);

(v) Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (A/HRC/13/37);

(w) World Customs Organization, International Air Transport Association and ICAO, *Guidelines on Advance Passenger Information* (Brussels, 2014);

(x) OSCE, Decision No. 6/06: Further measures to prevent the criminal use of lost/stolen passports and other travel documents, 2016;

(y) Global Counterterrorism Forum, "Good practices in the area of border security and management in the context of counterterrorism and stemming the flow of 'foreign terrorist fighters'";

(z) European Border and Coast Guard Agency, "Common core curriculum for border and coast guard basic training in the EU", 2017;

(aa) Fixed INTERPOL Network Database and Mobile INTERPOL Network Database;

(bb) INTERPOL I-24/7 secure global police communications system;

(cc) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and the Additional Protocol to the Convention, regarding supervisory authorities and transborder data flows;

(dd) Council of Europe, *Guidelines of the Committee of Ministers of the Council of Europe on human rights and the fight against terrorism* (Strasbourg, 2002).

(b) Movement of goods

332. The following international instruments, standards and good practices provide guidance in this area:

(a) Container Control Programme of UNODC and the World Customs Organization;

(b) Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction;

(c) ICAO, *Annex 9 to the Convention on International Civil Aviation: Facilitation* (Montreal, 2017), chapter 4, “Entry and departure of cargo and other articles”;

(d) World Customs Organization, *Global Information and Intelligence Strategy* (Brussels, 2005);

(e) World Customs Organization, *Customs Risk Management Compendium* (Brussels, 2011);

(f) World Customs Organization, *Coordinated Border Management Compendium* (Brussels, 2015);

(g) World Customs Organization, “Integrated supply chain management guidelines”, 2018;

(h) World Customs Organization, *SAFE Framework of Standards to Secure and Facilitate Global Trade* (Brussels, 2018);

(i) Global Counterterrorism Forum, “Good practices in the area of border security and management in the context of counterterrorism and stemming the flow of ‘foreign terrorist fighters’”.

(c) Civil aviation security

333. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principle 19;

(b) Addendum to the Madrid Guiding Principles, guiding principles 36–38;

(c) Convention on International Civil Aviation;

(d) Convention on Offences and Certain Other Acts Committed on Board Aircraft and the Protocol thereto;

(e) Convention for the Suppression of Unlawful Seizure of Aircraft and the Protocol thereto;

(f) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation and the Protocol thereto;

(g) ICAO, *Annex 9 to the Convention on International Civil Aviation: Facilitation* (Montreal, 2017);

(h) ICAO, *Annex 13 to the Convention on International Civil Aviation: Aircraft Accident and Incident Investigation* (Montreal, 2016);

(i) ICAO, *Annex 17 to the Convention on International Civil Aviation: Security* (Montreal, 2017);

(j) ICAO, *Aviation Security Manual* (Doc. 8973 – Restricted);

(k) ICAO, *Facilitation Manual* (Doc. 9957);

(l) ICAO, *Aviation Security Oversight Manual* (Doc. 10047);

(m) ICAO, *Manual on the Implementation of the Security Provisions of Annex 6* (Doc. 9811 – Restricted);

(n) ICAO, *Aerodrome Design Manual* (Doc. 9157);

(o) ICAO, *Aircraft Operations* (Doc. 8168);

(p) ICAO, *Airport Planning Manual* (Doc. 9184);

(q) ICAO, *Human Factors in Civil Aviation Security Operations* (Doc. 9808);

(r) ICAO, *Human Factors Training Manual* (Doc. 9683);

(s) ICAO, *Aviation Security Global Risk Context Statement* (Restricted);

(t) Counter-Terrorism Implementation Task Force working group on border management and law enforcement relating to counter-terrorism, "Risk management framework to support counter-terrorism objectives: coordinated border management in the air travel cycle";

(u) Convention on the Marking of Plastic Explosives for the Purpose of Detection;

(v) ICAO, ICAO Assembly resolution on addressing cybersecurity in civil aviation;

(w) ICAO, Standards and Recommended Practices and guidance material on protection of landside areas;

(x) ICAO, "Global Aviation Security Plan", 2017.

(d) Maritime security

334. The following international instruments, standards and good practices provide guidance in this area:

(a) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the Protocols thereto;

(b) International Convention for the Safety of Life at Sea, in particular chapter XI-2, "Special measures to enhance maritime security":

(i) Regulation XI-2/2, "International Ship and Port Facility Security Code", Part A;

(ii) Regulation XI-2/3, "Security levels";

(iii) Regulation XI-2/7, "Threats to ships";

(iv) Regulation XI-2/10, "Port facility security assessments";

(v) Regulation XI-2/12, "Equivalent security arrangements";

(vi) Regulation XI-2/13, "Communication of information.

(c) International Labour Organization (ILO) and IMO, Code of practice on security in ports;

(d) Seafarers' Identity Documents Convention (Revised), 2003;

(e) ILO, *Finger minutiae-based biometric profile for seafarers' identity documents* (Geneva, 2006), which gives guidelines for the incorporation of minutiae-based fingerprint biometric technology into seafarers' identity documents in accordance with the Seafarers' Identity Documents Convention;

(f) IMO, Maritime Security Circulars:

(i) Circular 1097, "Guidelines relating to the implementation of SOLAS chapter XI-2 and the ISPS Code";

(ii) Circular 1106, "Implementation of SOLAS chapter XI-2 and the ISPS Code to port facilities";

(iii) Circular 1110, "Matters related to SOLAS regulations XI-2/6 and XI-2/7";

(iv) Circular 1111, “Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code”;

(v) Circular 1132, “Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS Code”;

(vi) Circular 1154, “Guidance on training and certification for company security officers”;

(vii) Circular 1188, “Guidelines on training and certification for port facility security officers”;

(viii) Circular 1192, “Guidance on voluntary self-assessment by SOLAS contracting Governments and port facilities”;

(ix) Circular 1193, “Guidance on voluntary self-assessment by Administrations and for ship security”;

(x) Circular 1194, “Effective implementation of SOLAS chapter XI-2 and the ISPS Code”.

(e) Protection of critical infrastructure and soft targets

335. The following international instruments, standards and good practices provide guidance in this area:

(a) Council resolution 2341 (2017);

(b) Addendum to the Madrid Guiding Principles, guiding principle 50;

(c) European Commission, “European Programme for Critical Infrastructure Protection”, 2006;

(d) Treaty on Cooperation among the States Members of the Commonwealth of Independent States in Combating Terrorism, article 5, paragraph 1 (e);

(e) Inter-American Committee against Terrorism, Declaration on protection of critical infrastructure from emerging threats;

(f) OSCE, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace* (Vienna, 2013);

(g) Office of Counter-Terrorism and United Nations Counter-Terrorism Committee Executive Directorate, *The protection of critical infrastructures against terrorist attacks: compendium of good practices* (New York, 2018);

(h) Global Counterterrorism Forum, “Soft target protection initiative: Antalya memorandum on the protection of soft targets in a counterterrorism context”, 2017.

Chapter III. Security Council resolution 1373 (2001), paragraph 3

336. In paragraph 3 of its resolution 1373 (2001), the Security Council calls upon all States to:

(a) Find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups;

(b) Exchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts;

(c) Cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts;

(d) Become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999;

(e) Increase cooperation and fully implement the relevant international conventions and protocols relating to terrorism and Security Council resolutions 1269 (1999) and 1368 (2001);

(f) Take appropriate measures in conformity with the relevant provisions of national and international law, including international standards of human rights, before granting refugee status, for the purpose of ensuring that the asylum-seeker has not planned, facilitated or participated in the commission of terrorist acts;

(g) Ensure, in conformity with international law, that refugee status is not abused by the perpetrators, organizers or facilitators of terrorist acts, and that claims of political motivation are not recognized as grounds for refusing requests for the extradition of alleged terrorists.

A. Exchanging information

337. Member States should have in place procedures and mechanisms to encourage appropriate exchange of operational information by relevant law enforcement agencies. States should also be able to consult international and regional sources of law enforcement information in order to identify existing or potential foreign terrorist fighters. National law enforcement and security agencies should actively transmit relevant information that may be of use in identifying existing or potential foreign terrorist fighters.[301]

338. The Council has called on States to share, where appropriate, information about foreign terrorist fighters and other individual terrorists and terrorist organizations, including biometric and biographic information, via bilateral, regional and global law enforcement channels, and has stressed the importance of providing such information to national watch lists and multilateral screening databases. (For more information on biometric identification and watch lists and databases, see also chapter II, section O,

[301] Madrid Guiding Principles, guiding principle 15.

"Effective border security and related issues", subsection 16, "Biometric identification".)[302]

339. The Council has also called on States to consider, where appropriate, downgrading for official use intelligence threat data on foreign terrorist fighters and individual terrorists, to appropriately provide such information to front-line screeners, such as immigration, customs and border security officials, and to appropriately share such information with other concerned States and relevant international organizations, in compliance with international and national law and policy.[303]

340. In its resolution 2341 (2017), on the protection of critical infrastructure from terrorist attacks, the Council recognizes that protection efforts entail multiple streams of efforts, such as planning; public information and warning; operational coordination; intelligence and information-sharing; interdiction and disruption; screening, search and detection; access control and identity verification; cybersecurity; physical protective measures; risk management for protection programmes and activities; and supply chain integrity and security. The Council also calls on States to explore ways to exchange relevant information and to cooperate actively in the prevention, protection, mitigation, preparedness, investigation, response to or recovery from terrorist attacks planned or committed against critical infrastructure.

341. In its resolution 2396 (2017), the Council calls upon Member States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks against soft targets, and urges States able to do so to assist in the delivery of effective and targeted capacity development, training and other necessary resources, and technical assistance, where it is needed to enable all States to develop appropriate capacity to implement contingency and response plans with regard to attacks on soft targets.

342. Member States bear the primary responsibility for the protection of critical infrastructure and soft targets. Each State defines critical infrastructure and soft targets in accordance with its specific national context. However, there is a growing need to increase cooperation among States and with private companies that own, operate and manage critical infrastructure and soft targets in order to address security needs, reduce vulnerabilities and share information on threats, vulnerabilities and measures to mitigate the risk. Joint training, communications networks and early warning mechanisms should be utilized and improved. In order for public-private partnerships to maximize their potential to protect soft targets, such partnerships need to be developed and fostered at the national level, as well as at the local or city level. Member States should encourage and support such partnerships with companies, which can contribute to protection, mitigation, investigation, response and recovery from damage from terrorist attacks against soft targets and should involve local authorities in those efforts.

343. The Council has recognized the proven effectiveness of the I-24/7 secure global police communications system and encouraged States to increase the capacity of their National Central Bureaus to utilize it and to designate a round-the-clock point of contact for the system.[304]

344. The Council has also encouraged States to consider extending access to and, where appropriate, integrate into their national systems, the I-24/7 system, beyond

[302] Resolution 2322 (2016), para. 3.
[303] Ibid., para. 5.
[304] Ibid., para. 16.

National Central Bureaus to other national law enforcement entities at strategic locations such as remote border crossings, airports, customs and immigration posts or police stations.[305]

345. The Council has called upon Member States to intensify and accelerate the timely exchange of relevant operational information and financial intelligence regarding actions, movements and patterns of movements of terrorists or terrorist networks, including in the context of potential linkages that may exist between terrorism and organized crime. Member States shall consider establishing laws and mechanisms that allow for international cooperation, including the use of joint investigation mechanisms and enhanced coordination of cross-border investigations in cases related to the linkages between terrorism and organized crime, whether domestic or transnational.[306]

346. Based on observations made during the Committee's comprehensive and focused country visits, the reports of Member States to the Committee on their implementation of resolution 1373 (2001) and the Madrid Guiding Principles, the following practices encourage appropriate exchange of information:

(a) A national counter-terrorism strategy that comprises international cooperation, intelligence-sharing and coordination at the national, regional and global levels;

(b) Procedures and tools for international police and customs cooperation (e.g., databases, secure communication systems), operational 24 hours a day, seven days a week, including mechanisms to alert law enforcement agencies to INTERPOL-United Nations Security Council Special Notices for individuals and entities subject to United Nations sanctions, for instance because of their affiliation with Al-Qaida;

(c) The maintenance of a sufficiently comprehensive integrated counter-terrorism database;

(d) The network of INTERPOL National Central Bureaus, the World Customs Organization's network of Regional Intelligence Liaison Offices, membership of INTERPOL and regional law enforcement groups or associations, and other multilateral, bilateral and regional networks;

(e) Focal points for the purpose of information exchange and cooperation;

(f) System or process for the communication and transmittal of information, operating 24 hours a day, seven days a week;

(g) Joint investigation teams between two or more States, as required, on the basis of legal agreements;

(h) A regional arrest warrant to facilitate extradition between States within a region, where applicable;

(i) Consultation with other Member States' intelligence and security services, including through regional forums;

(j) A dedicated programme to coordinate and cooperate actively, at the national and regional levels, in the prevention, protection, mitigation, preparedness, investigation, response to or recovery from terrorist attacks planned or committed against critical infrastructure and soft targets;

(k) Cooperative measures to work with INTERPOL in monitoring and preventing the transit of terrorists, including foreign terrorist fighters, including by

[305] Ibid., para. 17.

[306] Resolution 2482 (2019), para. 2 and 15 (b).

extending access to the I-24/7 system to counter-terrorism units and other relevant law enforcement agencies with a counter-terrorism mandate. States should also actively contribute to the population of INTERPOL operational databases, including those on known terrorists, foreign terrorist fighters, stolen and lost travel documents and stolen firearms and explosives;

(l) Safeguards linked to the right to privacy and presumption of innocence, as well as practices that collect, store and share information in a non-discriminatory manner consistent with international human rights law.

347. The following issues should be considered:

(a) Do law enforcement agencies cooperate, coordinate and exchange information with counterparts in other States?

(b) Is the national police force an active member of a regional network of law enforcement agencies?

(c) Does the State seek to engage, in addition to formal means of cooperation, in informal (police-to- police) cooperation through multilateral and bilateral channels in order to foster real-time exchange of information?

(d) Does the State collect biometric and biographic information and, if so, does it share such information via bilateral, regional and global law enforcement channels and provide such information to national watch lists and multilateral screening databases?

(e) Does the State exercise downgrading for official use intelligence threat data on foreign terrorist fighters and individual terrorists? If so, is such information available to front-line screeners, such as immigration, customs and border security officers, and does the State share such information with other concerned States and relevant international organizations?

(f) Is there a designated 24 hours a day, seven days a week point of contact for law enforcement communication and cooperation in countering terrorism and foreign terrorist fighters?

(g) Does the State maintain an integrated counter-terrorism database that includes input from authorized and relevant law enforcement agencies?[307]

(h) Is the integrated counter-terrorism database sufficiently comprehensive? Does it include information from abroad? Is the database accessible by all relevant law enforcement agencies?

(i) Does the database contain information from INTERPOL?[308]

(j) Does the State alert law enforcement agencies to INTERPOL-United Nations Security Council Special Notices for individuals and entities subject to United Nations sanctions, for instance because of their affiliation with Al-Qaida?[309]

(k) Are the databases connected to the I-24/7 system?[310]

(l) Are law enforcement agencies equipped with the legal and operational mechanisms required to engage in international cooperation against terrorism?[311]

[307] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 3.1.1.
[308] Ibid., 3.1.2.
[309] Ibid., 3.1.3.
[310] Ibid., 3.1.4
[311] Ibid., 3.2.1

(m) Are the State's law enforcement agencies equipped with bilateral and multilateral tools for cooperation in investigations related to acts of terrorism and terrorist organizations?[312]

(n) Are all the relevant law enforcement agencies with a counter-terrorism mandate able to access the INTERPOL police databases on known terrorists (including foreign terrorist fighters), stolen and lost travel documents, stolen firearms and so forth, available via the I-24/7 system?

(o) Are there procedures and tools in place to ensure access to the aforementioned databases by front-line law enforcement officers, as well as at border entries and departure points?[313]

(p) Are there measures and procedures in place to actively populate international police databases such as the INTERPOL police databases?[314]

(q) Are the relevant law enforcement agencies making use of the World Customs Organization's Customs Enforcement Network secure platform and the network of Regional Intelligence Liaison Offices?

348. Member States should strive to have in place databases and related information-sharing procedures and mechanisms related to the following:

(a) Information-sharing related to terrorists and transnational organized crime;[315]

(b) Information-sharing for the purpose of identifying smuggling routes (such as those used by ISIL (Da'esh) and Jabhat Fath al-Sham);[316]

(c) The sharing of operational information regarding trafficking in arms;[317]

(d) Information-sharing mechanisms, especially cross-border customs cooperation and networks for information-sharing, to prevent the illicit transfer, accumulation and misuse of small arms and light weapons;[318]

(e) The sharing of information, including operational information, on suspected traffickers and trafficking routes for small arms and light weapons;[319]

(f) Data collection and national risk assessment criteria concerning how women and children are impacted by the illicit proliferation of small arms and light weapons;[320]

(g) Information-sharing capabilities and practices within and between Governments to effectively counter the financing of terrorism;[321]

(h) The exchange of information regarding actions or movements of terrorists or terrorist networks, including foreign terrorist fighters, through bilateral or multilateral mechanisms,[322] including the sharing of best practices and improved understanding of foreign terrorist fighter travel patterns;[323]

---

[312] Ibid., 3.2.2.
[313] Madrid Guiding Principles, guiding principle 17.
[314] Ibid., guiding principle 15.
[315] Resolution 2195 (2014), para. 8.
[316] Resolution 2199 (2015), para. 14.
[317] Ibid., para. 24.
[318] Resolution 2220 (2015), para. 1.
[319] Ibid., paras. 11 and 19.
[320] Ibid., para. 16.
[321] Resolution 2253 (2015), para. 25.
[322] Resolution 2178 (2014), para. 3.
[323] Ibid., para. 11.

(i) Are law enforcement agencies able to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks against critical infrastructure and soft targets, including through:

(i) Bilateral and multilateral means of information-sharing?

(ii) Risk assessment and joint law enforcement?

(iii) Joint training?

(iv) Use or establishment of relevant communication?

(v) Emergency warning networks?

349. For issues relating to advance passenger information and watch lists, see also chapter II, section O, "Effective border security and related issues", subsection 5, "Screening prior to arrival in the destination State". For issues relating to small arms and light weapons, see also chapter II, section C, "Eliminating the supply of weapons to terrorists".

350. The following international instruments, standards and good practices provide guidance in this area:

(a) Guidelines for reporting on the implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects;

(b) UNODC, *Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocol Thereto* (New York, 2004);

(c) INTERPOL fact sheet COM/FS/2016-03/GI-04;

(d) INTERPOL fact sheet COM/FS/2015-02/GI-03;

(e) Madrid Guiding Principles, guiding principles 15, 17 and 19;

(f) Treaty on Cooperation among the States Members of the Commonwealth of Independent States in Combating Terrorism, article 11;

(g) Shanghai Cooperation Organization Convention against Terrorism, article 11.

B. Multilateral and bilateral agreements

351. In paragraph 3 (b) of resolution 1373 (2001), the Council calls on States to cooperate on judicial matters. The Council identifies bilateral and multilateral arrangements and agreements as effective methods of facilitating international cooperation.[324] Moreover, the creation of judicial cooperation networks has shown the utility of regional mechanisms in enhancing formal and informal cooperation.[325]

352. In paragraph 2 (b) of its policy guidance on international cooperation, issued in 2010, the Counter-Terrorism Committee encourages States to increase their bilateral cooperation on extradition and mutual legal assistance and to share information about the process and results of mutual legal assistance. Member States are also called upon to become parties to relevant subregional and regional instruments on those matters[326] and to implement regional and international best practices.[327] The Madrid Guiding

[324] Resolution 1373 (2001), para. 3 (e).
[325] S/2016/501, para. 54.
[326] Counter-Terrorism Committee, "Policy guidance on international cooperation", para. 2 (c).
[327] Ibid., para. 2 (f).

Principles encourage States to consider developing and participating in regional mutual legal assistance cooperation platforms to address the foreign terrorist fighter threat.

353. The following issues should be considered:

(a) Has the State concluded bilateral agreements with other States on legal cooperation matters, especially extradition and mutual legal assistance? (See also chapter II, section N, “International legal cooperation”.)[328]

(b) Has the State ratified the relevant multilateral treaties on organized crime, drug trafficking, human rights and other issues related to the fight against terrorism?[329]

(c) Has the State considered establishing multilateral, regional or bilateral treaties as a legal basis to determine the content of a request for mutual legal assistance?[330]

(d) Has the State concluded bilateral agreements with other States on criminal matters?[331]

(e) Does the State rely on bilateral or multilateral treaties regulating the execution of search and seizure of evidence in another State?[332]

(f) Has the State considered establishing bilateral exchanges with interested States to clarify delisting petition issues?[333]

(g) Has the State considered establishing bilateral or multilateral agreements for the sharing of the proceeds of crime on a regular or case-by-case basis?[334]

(h) Does the State, as State of destination, origin or transit, plan to conclude bilateral agreements on the transfer of foreign terrorist fighters to the States of their nationality?[335]

(i) Does the State work closely with regional organizations to strengthen judicial and other relevant networks and cross-regional cooperation?[336]

354. The following international instruments, standards and good practices provide guidance in this area:

(a) Counter-Terrorism Committee, “Policy guidance on international cooperation: policy guidance PG.3”, June 2010;

(b) UNODC, *Manual on International Cooperation in Criminal Matters related to Terrorism* (New York, 2009), modules 1 and 2.

C. Ratifying the international counter-terrorism instruments

355. In paragraph 3 of its resolution 1373 (2001), the Council calls on States to become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the

[328] Ibid., para. 2 (b).
[329] Global Counterterrorism Forum, Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector.
[330] UNODC, Manual on International Cooperation, module 2.D.1., p. 113.
[331] Ibid., module 1.B.4., p. 21.
[332] Ibid., module 2.B.3., p. 84.
[333] Ibid., module 2.B.3., p. 103.
[334] Ibid., module 2.C.7., p. 111.
[335] S/2015/975, para. 43.
[336] Ibid., para. 159 (b).

Suppression of the Financing of Terrorism. In 2010, the Counter-Terrorism Committee, in paragraph 2 (a) of its policy guidance on international cooperation, reiterated that requirement.

356. With regard to the international counter-terrorism instruments, resolution 1373 (2001) contains two distinct requirements. Paragraph 2 (e) obliges all Member States to ensure that terrorist acts are established as serious criminal offences in domestic law. (This aspect of the resolution is addressed in chapter II, section G, "Codification".) Paragraph 3 of the resolution calls on States to become parties to and implement the international instruments. As some elements of the instruments are non-criminal in nature, it is not adequate simply to assess criminalization. For example, neither the Convention on Offences and Certain Other Acts Committed on Board Aircraft nor the Convention on the Marking of Plastic Explosives for the Purpose of Detection create criminal offences, but their status of implementation by States must be assessed.

Convention on Offences and Certain Other Acts Committed on Board Aircraft

357. With regard to the powers of the aircraft commander, the following issues should be considered:

(a) Has the State put in place measures to confer special powers to the commander of an aircraft in respect of offences or acts committed, or about to be committed, by a person on board an aircraft in flight in the airspace of a party other than the State of registration, that is, in foreign airspace?

(b) Has the State put in place measures to confer special powers to the commander of an aircraft in respect of offences or acts committed, or about to be committed, by a person on board an aircraft in flight in the airspace of the State of registration?

(c) Has the State put in place measures to confer special powers to the commander of an aircraft in respect of offences or acts committed, or about to be committed, by a person on board an aircraft in flight over the high seas or any other area outside the territory of the State, if:

(i) The last point of take-off or the next place of intended landing is situated in a State other than that of registration?

(ii) The aircraft subsequently flies in the airspace of a State other than that of registration?

(d) Does the State allow the commander of an aircraft – when the commander has reasonable grounds to believe that a person has committed, or is about to commit, on board the aircraft an offence or act contemplated by the Convention – to impose reasonable measures, including restraint, as are necessary to protect the safety of the aircraft or of persons or property on board?

(e) Does the State allow the commander of an aircraft – when the commander has reasonable grounds to believe that a person has committed, or is about to commit, on board the aircraft an offence or act contemplated by the Convention – to impose reasonable measures, including restraint, as are necessary to maintain good order and discipline on board?

(f) Does the State allow the commander of an aircraft to deliver a person to competent authorities when the commander has reasonable grounds to believe that this person has committed, or is about to commit, on board the aircraft an offence or act contemplated by the Convention?

(g) Does the State allow the commander of an aircraft to disembark a person when the commander has reasonable grounds to believe that this person has committed, or is about to commit, on board the aircraft an offence or act contemplated by the Convention?

(h) Does the State have all measures in place to enable the commander to require or authorize the assistance of other crew members to restrain any person whom he or she is entitled to restrain?

(i) Does the State have all measures in place to enable the commander to request (but not require) or authorize the assistance of passengers to restrain any person whom he or she is entitled to restrain?

(j) Does the State have all measures in place to enable any crew member or passenger to take reasonable preventive measures without the authorization of the commander when he or she has reasonable grounds to believe that such action is immediately necessary to protect the safety of the aircraft or of persons or property on board?

(k) Can the State ensure that neither the commander, nor the members of the crew, the passengers, the owner or operator of the aircraft, nor the person on whose behalf the flight was performed, is to be held responsible for actions taken in accordance with the Convention in any proceedings on account of the treatment undergone by the person against whom the actions were taken?

358. With regard to the unlawful seizure of aircraft, the following issue should be considered: Is the State able to take all appropriate measures to restore control of the aircraft to its lawful commander or to preserve his or her control of the aircraft when a person on board an aircraft has unlawfully committed by force, or threat of force, an act of interference, seizure or other wrongful exercise of control of an aircraft in flight, or when such an act is about to be committed?[337, 338]

359. With regard to the powers and duties of parties in relation to disembarkation and delivery, the following issues should be considered:[339]

(a) Does the State pay due regard to the safety and other interests of air navigation when taking any measures for investigation or arrest, or otherwise exercising jurisdiction, in connection with any offence committed on board an aircraft?

(b) Do the State's authorities have all procedures in place to receive from the commander the notification of the fact that a person on board is under restraint, and why?

(c) Has the State allowed the commander of an aircraft registered with another party to disembark a person on its own territory if its territory is where the aircraft lands?

(d) Does the State take delivery of any person who the commander delivers?

360. With regard to the treatment of other passengers and the crew, the following issues should be considered:[340]

[337] Commonwealth Secretariat, *Implementation Kits for the International Counter-Terrorism Conventions* (London, 2002), chap. 2, p. 17.

[338] UNODC, *Guide for the Legislative Incorporation and Implementation of the Universal Anti-Terrorism Instruments* (New York, 2006), p. 76.

[339] Commonwealth Secretariat, *Implementation Kits*, chap. 2, pp. 17–18.

[340] Ibid., chap. 2, p. 18.

(a) In the case of the unlawful seizure of an aircraft, is the State able to take appropriate measures to permit the passengers and crew to continue their journey as soon as practicable?[341]

(b) Can the State ensure that it is able to accord to a person who wants to continue the journey a treatment which is no less favourable for protection and security than that accorded to nationals of the State in like circumstances?

International Convention against the Taking of Hostages[342]

361. The following issues should be considered:

(a) Is the State able to take all measures it considers appropriate to ease the situation of the hostage being held and, in particular, to secure release and aid with departure?

(b) Did the State return as soon as possible to the former hostage any object which an offender obtained as a result of the hostage-taking and which came into the custody of the State?

Convention on the Physical Protection of Nuclear Material[343]

362. The following issues should be considered:

(a) Can the State – as exporting State or State authorizing the export of the nuclear material – ensure that the nuclear material is not exported unless the State has received assurances that during international nuclear transport the nuclear material will be protected at the levels described in annex 1 to the Convention?

(b) Can the State ensure that nuclear material is not imported into its territory from a non-State party without an assurance that during international nuclear transport it will be protected at the levels described in annex 1 to the Convention?

(c) Does the State apply the same protection when nuclear material is transported from one part of its territory to another part of it through international waters or airspace?

Amendment to the Convention on the Physical Protection of Nuclear Material

363. The following issues should be considered:

(a) Does the State protect nuclear facilities and material in peaceful domestic use, storage and transport?

(b) Does the State participate in expanded cooperation with other States regarding rapid measures to:

(i) Locate and recover stolen or smuggled nuclear material;

(ii) Mitigate any radiological consequences or sabotage;

(iii) Prevent and combat related offences?

[341] UNODC, *Guide for the Legislative Incorporation*, p. 76.
[342] Commonwealth Secretariat, *Implementation Kits*, chap. 7, p. 147.
[343] Ibid., chap. 8, p. 165.

Convention on the Marking of Plastic Explosives for the Purpose of Detection

364. The following issue should be considered: Is the State able to destroy all unmarked explosives in its territory or render them ineffective within a period of 3 to 15 years from the entry into force of the Convention?[344]

International Convention for the Suppression of the Financing of Terrorism[345]

365. The following issues should be considered:

(a) Has the State taken appropriate measures for the identification, detection and freezing or seizure of funds used or allocated for the purpose of committing financing offences and for the eventual forfeiture of such funds (see also chapter I)?

(b) Has the State taken appropriate measures for the identification, detection and freezing or seizure of any funds derived from or obtained, directly or indirectly, through the commission of a financing offence (see also chapter I)?

(c) Has the State entered into bilateral agreements on the sharing of funds derived from forfeitures (see also chapter I)?

(d) Has the State established mechanisms by which forfeited funds could be used to compensate victims of terrorism?

(e) Can the State ensure that the above measures can be carried out without prejudice to the rights of third parties?

2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation

366. The following issue should be considered: Does the State have legislation enabling a legal entity to be held civilly, administratively or criminally liable when a person responsible for its management or control has, in that capacity, committed an offence established by the Convention?[346]

367. The following international instruments, standards and good practices provide guidance in this area:

(a) UNODC, *Guide for the Legislative Incorporation and Implementation of the Universal Anti-Terrorism Instruments* (New York, 2006);

(b) UNODC, *Legislative Guide to the Universal Legal Regime against Terrorism* (Vienna, 2008);

(c) Commonwealth Secretariat, *Implementation Kits for the International Counter-Terrorism Conventions* (London, 2002).

D. Measures with respect to refugees and asylum

368. In its resolution 1373 (2001), the Council calls upon States to take appropriate measures to ensure that persons who have planned, facilitated or participated in the commission of terrorist acts are not granted refugee status and that refugee status is not abused by the perpetrators, organizers or facilitators of such acts.[347] In its resolution 2178 (2014), the Council calls on States to also take such measures with respect to foreign terrorist fighters. Such measures, as with all measures taken to counter

[344] UNODC, *Legislative Guide to the Universal Legal Regime against Terrorism* (Vienna, 2008).
[345] Resolution 1373 (2001), para. 3 (f)–(g).
[346] Resolution 2178 (2014).
[347] See also resolution 2322 (2016), para. 10.

terrorism, must comply with international law, including international human rights and refugee law.[348] The Council reiterated those calls in its resolution 2322 (2016).

369. The Convention relating to the Status of Refugees establishes clear criteria for determining who is a refugee and is therefore entitled to international protection. It also stipulates that such protection shall not be afforded to any person where there are serious reasons for considering that he or she has committed a war crime, a crime against humanity or a serious non-political crime, or is guilty of acts contrary to the purposes and principles of the United Nations.

370. However, States often encounter difficulties in identifying such persons in a timely manner, in particular in situations of large-scale flows of migrants, refugees and asylum seekers. A robust capacity to receive, register and screen arrivals can support counter-terrorism efforts by enabling States to distinguish between different categories of persons and by allowing for the early identification of individuals who may pose a security risk.

371. International refugee law further stipulates that refugees are bound to abide by the laws of their host country. They are not immune from prosecution for any crimes committed on the territory of the host country and their status does not preclude appropriate measures where an individual is found to pose a security risk.[349] The Convention relating to the Status of Refugees includes express provisions that permit the expulsion of refugees on grounds of national security or public order under certain circumstances.

372. The Council has emphasized the obligation of non-refoulement, as enshrined in the Convention relating to the Status of Refugees. Pursuant to article 33 of the Convention, no State "shall expel or return ("refouler") a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion", although the benefit of that provision "may not, however, be claimed by a refugee whom there are reasonable grounds for regarding as a danger to the security of the country in which he is, or who, having been convicted by a final judgment of a particularly serious crime, constitutes a danger to the community of that country". Independently of those provisions, human rights law imposes an absolute prohibition on returning an individual to a State where there are substantial grounds for believing that he or she might be subjected to torture. That prohibition applies irrespective of whether that individual has sought, or been granted, refugee status.

373. The following issues should be considered:

(a) Is the State a party to the Convention relating to the Status of Refugees and the Protocol thereto?

(b) Does the State have in place a system for determining refugee status?[350]

(c) Does the State have in place the necessary legal provisions and procedures to ensure respect for the principle of non-refoulement and other human rights limitations to extradition and expulsion, such as substantial risk of human rights violations if a suspect is extradited or expelled?[351]

[348] Resolution 1624 (2005), preamble.

[349] Ibid., preamble; Convention Relating to the Status of Refugees, art. 33 (2); and Organization of African Unity Convention Governing the Specific Aspects of Refugee Problems in in Africa.

[350] S/2015/975, para. 41.

[351] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 3.4.3; resolution 1373 (2001); S/2015/975; and S/2016/49.

(d) Are border officials trained to identify refugees and refer them to the appropriate authorities?

(e) Does the State have in place procedures for dealing with large-scale influxes of migrants, refugees and asylum seekers?[352]

(f) Does the procedure for determining refugee status prevent the granting of asylum to an individual who has planned, facilitated or participated in a terrorist act?[353]

(g) Does the State's asylum law provide for the revocation of refugee status where an individual granted that status is subsequently involved in acts criminalized under the international counter-terrorism instruments?[354]

(h) Does the State have a specialized exclusion unit within the agency responsible for determining refugee status to carry out these specialized assessments?[355]

(i) Are exclusion and expulsion procedures for asylum seekers and refugees in compliance with international human rights standards and appropriate safeguards, including:

(i) Right to respond to evidence or information;

(ii) Right to legal assistance;

(iii) Right to an interpreter;

(iv) Right to appeal and to protection against removal until all legal remedies have been exhausted.[356]

(j) Where persons are excluded from refugee status (or have that status revoked) for involvement in terrorist-related acts, does the State refer the cases to its prosecuting authorities in accordance with the international counter-terrorism instruments, where appropriate?[357]

(k) Does the State issue secure machine readable travel documents to recognized refugees?[358]

374. For issues relating to people who may have been guilty of incitement to commit a terrorist act, see also chapter IV, section B, "Measures with respect to entry and asylum screening for people who may have been guilty of incitement to commit a terrorist act".

375. The following international instruments, standards and good practices provide guidance in this area:

(a) Convention relating to the Status of Refugees and the Protocol thereto;

(b) International Covenant on Civil and Political Rights;

(c) Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment;

---

[352] UNHCR, "Addressing security concerns without undermining refugee protection", Rev.2, 17 December 2015.

[353] Ibid.

[354] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 3.4.4.

[355] Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, art. 7; International Convention against the Taking of Hostages, art. 8; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, art. 10; International Convention for the Suppression of Terrorist Bombings, art. 7; and International Convention for the Suppression of the Financing of Terrorism, art. 10.

[356] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 3.4.5.

[357] Resolution 1373 (2001).

[358] Counter-Terrorism Committee Executive Directorate, detailed implementation survey, template 3.5.1.

(d) Organization of African Unity Convention Governing the Specific Aspects of Refugee Problems in Africa;

(e) Convention on the Reduction of Statelessness;

(f) Counter-Terrorism Implementation Task Force, *Basic Human Rights Reference Guide: The Stopping and Searching of Persons* (New York, 2010);

(g) UNHCR, *Handbook and Guidelines on Procedures and Criteria for Determining Refugee Status under the 1951 Convention and the 1967 Protocol relating to the Status of Refugees* (Geneva, December 2011);

(h) UNHCR, "Addressing security concerns without undermining refugee protection", Rev.2, 17 December 2015;

(i) UNHCR, *Refugee Protection and Mixed Migration: The 10-Point Plan in Action* (Geneva, 2016);

(j) Convention for the Protection of Human Rights and Fundamental Freedoms.

E. Non-application of the "political offence" doctrine

376. In paragraph 3 (g) of resolution 1373 (2001), the Council calls on States to ensure that, in conformity with international law, claims of political motivation are not recognized as grounds for refusing requests for the extradition of alleged terrorists. Legislation providing that terrorist offences that qualify as terrorist acts under international legal norms and principles will not be considered excused or exempt from international cooperation on grounds that they are political should therefore be in place. That requirement should be distinguished from the parallel obligation of States to refuse cooperation where it is evident that the transfer of an individual is being requested for the purpose of improper prosecution.

377. The following issue should be considered: Are terrorism offences excluded from offences of a political nature for which extradition or mutual legal assistance in criminal matters may be refused?

F. Denying cooperation on grounds of improper prosecution

378. The international counter-terrorism instruments address this requirement. For example, article 15 of the International Convention for the Suppression of the Financing of Terrorism states that "Nothing in this Convention shall be interpreted as imposing an obligation to extradite or to afford mutual legal assistance, if the requested State Party has substantial grounds for believing that the request for extradition [or for mutual legal assistance] has been made for the purpose of prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin or political opinion or that compliance with the request would cause prejudice to that person's position for any of these reasons". It is possible, in such cases, that the affected person would have a legitimate claim to refugee status.

379. The following issue should be considered: Are there legal provisions in place to refuse extradition where there are substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin or political opinion, or that compliance with the request would cause prejudice to that person's position for any of these reasons?

Chapter IV. Security Council resolution 1624 (2005)

380. In its resolution 1624 (2005), the Security Council calls upon all States to:

(a) Adopt such measures as may be necessary and appropriate and in accordance with their obligations under international law to:

(i) Prohibit by law incitement to commit a terrorist act or acts;

(ii) Prevent such conduct;

(iii) Deny safe haven to any persons with respect to whom there is credible and relevant information giving serious reasons for considering that they have been guilty of such conduct;

(b) Cooperate, inter alia, to strengthen the security of their international borders, including by combating fraudulent travel documents and, to the extent attainable, by enhancing terrorist screening and passenger security procedures with a view to preventing those guilty of incitement to commit a terrorist act or acts from entering their territory;

(c) Continue international efforts to enhance dialogue and broaden understanding among civilizations, in an effort to prevent the indiscriminate targeting of different religions and cultures, and to take all measures as may be necessary and appropriate and in accordance with their obligations under international law to counter incitement of terrorist acts motivated by extremism and intolerance and to prevent the subversion of educational, cultural and religious institutions by terrorists and their supporters;

(d) Ensure that any measures taken to implement the subparagraphs above comply with all of their obligations under international law, in particular international human rights, refugee and humanitarian law.

A. Preventing and countering incitement and recruitment to commit terrorist acts, consistent with international law

381. The Council, in paragraph 1 of resolution 1624 (2005), calls upon all States to adopt such measures as may be necessary and appropriate and in accordance with their obligations under international law to prohibit by law incitement to commit a terrorist act or acts, prevent such conduct and, in paragraph 3, to take measures to counter incitement of terrorist acts motivated by extremism and intolerance.

382. In the resolution, the Council also calls upon all States to deny safe haven to any persons about whom there is credible and relevant information giving serious reasons for considering that they have been guilty of such incitement, and to strengthen international cooperation, including through enhanced border security and screening measures, with a view to preventing those guilty of such incitement from entering their territories.

383. In its resolution 2396 (2017), the Council recognizes that a comprehensive approach to the threat posed by foreign terrorist fighters requires addressing the conditions conducive to the spread of terrorism, including by preventing radicalization to terrorism; stemming recruitment; disrupting financial support to terrorists; countering incitement to commit terrorist acts; promoting political and religious tolerance, good governance, economic development, social cohesion and inclusiveness; ending and resolving armed conflicts; and facilitating investigation, prosecution, reintegration and rehabilitation. The Council urges Member States and the United Nations system to take measures, pursuant to international law, to address, in a balanced manner, all internal and external drivers of violent extremism that is conducive to terrorism, in accordance with the United Nations Global Counter-Terrorism Strategy.

384. States face a significant threat from the abuse of ICTs for terrorist purposes. The exploitation of ICT – and of the Internet and social media platforms in particular – has notably enabled terrorists to transmit their propaganda, share training materials, engage in the illicit trade in weapons, identify potential recruits, generate funds and carry out attacks. Messages are conveyed through not only mainstream social media applications but also encrypted channels and the dark web.

385. States, regional organizations, the private sector and civil society should establish effective partnerships with a view to developing improved methods for monitoring and studying terrorist content transmitted over the Internet and other communications technologies and countering incitement to commit terrorist acts, utilizing it for intelligence purposes and referring it, where appropriate, to relevant law enforcement agencies. Counter-narratives and positive messaging can also be effective measures.

386. States must ensure that any measures taken to implement resolution 1624 (2005) comply with all their obligations under international law, in particular international human rights, refugee and humanitarian law.[359]

387. In developing effective measures to address incitement and promote dialogue, States should consider the roles of women in the context of promoting and inciting terrorism, as well as in countering terrorist narratives, and develop appropriate capacity-building measures to address this phenomenon.

388. The following issues should be considered:

(a) Does the State have in place clear and precise legislation prohibiting incitement to commit a terrorist act or acts?[360]

(b) Do the legislation and related measures comply with the States' obligation to ensure respect for the right to freedom of expression, as recalled in the preamble to resolution 1624 (2005), and furthermore take into account that any restrictions thereon shall only be such as are provided by law and are necessary on the grounds set out in paragraph 3 of article 19 of the International Covenant on Civil and Political Rights?

(c) What examples can the State provide to show that it sought to prevent incitement to commit a terrorist act or acts through law enforcement strategies or other measures?[361]

(d) What steps has the State taken to prevent terrorists from exploiting ICTs, in particular the Internet?[362]

(e) Does the State act cooperatively with other States to prevent terrorists from exploiting sophisticated technology, communications and resources to incite support for terrorist acts?[363]

(f) Has the State established partnerships with international and regional organizations, the private sector and civil society to improve methods for monitoring and studying terrorist content transmitted over the Internet and other communications technologies, utilizing it for intelligence work and referring it, where appropriate, to relevant law enforcement agencies?[364]

---

[359] Counter-Terrorism Committee Executive Directorate, detailed implementation survey for resolution 1624 (2005), template 1.

[360] Ibid., template 3.

[361] Global survey of the implementation of Security Council resolution 1624 (2005) by Member States (S/2016/50, annex), para. 16.

[362] Counter-Terrorism Committee Executive Directorate, detailed implementation survey for resolution 1624 (2005), template 7.

[363] Resolution 2178 (2014), para. 11.

[364] Resolution 1624 (2005).

B. Measures with respect to entry and asylum screening for people who may have been guilty of incitement to commit a terrorist act

389. Pursuant to resolution 1624 (2005), all States are called upon to adopt measures to deny safe haven to any person with respect to whom there is credible and relevant information giving serious reasons for considering that they have been guilty of incitement to commit a terrorist act.

390. In the preamble to the resolution, the Council recalls the right to seek and enjoy asylum reflected in article 14 of the Universal Declaration of Human Rights. It reaffirms that the acts, methods and practices of terrorism are contrary to the purposes and principles of the United Nations and that the protections afforded by the Convention relating to the Status of Refugees and its Protocol shall not extend to any persons guilty of such acts. (For a discussion on asylum processes and the application of the Convention's exclusion clauses, see also chapter III, section D, "Measures with respect to refugees and asylum".)

391. As for other aspects of border management, international cooperation is critical. In paragraph 2 of resolution 1624 (2005), the Council calls upon all States to cooperate with other States, inter alia, to strengthen the security of their international borders, including by combating fraudulent travel documents and, to the extent attainable, by enhancing terrorist screening and passenger security procedures with a view to preventing those guilty of incitement to commit a terrorist act or acts from entering their territory. Border control and passenger screening is particularly relevant in the case of foreign terrorist fighters who may seek asylum in, or entry into, a Member State.

392. The following issues should be considered:

(a) Does the State have in place measures facilitating the denial of safe haven to any persons with respect to whom there is credible and relevant information giving serious reasons for considering that they have been guilty of incitement to commit a terrorist act or acts?[365]

(b) Does the State cooperate with other States, inter alia, to strengthen the security of its international borders, including by combating fraudulent travel documents and, to the extent attainable, by enhancing terrorist screening and passenger security procedures with a view to preventing those guilty of incitement to commit a terrorist act from entering their territory?[366]

(c) Does the State employ evidence-based traveller risk assessment and screening procedures, including collection and analysis of travel data, without resorting to profiling based on stereotypes founded on grounds of discrimination prohibited by international law?[367]

(d) Does the State safeguard the right to seek and enjoy asylum while ensuring that asylum is not extended to any person with respect to whom there are serious

[365] Ibid., para. 1 (c).

[366] Ibid., para. 2.

[367] Ibid., paras. 2 and 4; Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: ten areas of best practices in countering terrorism (A/HRC/16/51), paras. 29–32. In his report, the Special Rapporteur formulates the model offence of incitement to terrorism as follows: "It is an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed." See also Universal Declaration of Human Rights, art. 7.

reasons for considering that he or she has been guilty of incitement to commit a terrorist act, as properly defined?[368]

393. For issues relating to the security of international borders, see also chapter II, section O, "Effective border security and related issues"; for issues relating to the exchange of information regarding actions or movements of terrorists, see also chapter III, section A, "Exchanging information".

394. The following international instruments, standards and good practices provide guidance in this area:

(a) UNHCR, *Handbook and Guidelines on Procedures and Criteria for Determining Refugee Status under the 1951 Convention and the 1967 Protocol relating to the Status of Refugees* (Geneva, December 2011);

(b) UNHCR, "Addressing security concerns without undermining refugee protection", Rev.2, 17 December 2015;

(c) UNHCR, *Refugee Protection and Mixed Migration: The 10-Point Plan in Action* (Geneva, 2016);

(d) Madrid Guiding Principles;

(e) Universal Declaration of Human Rights, article 14;

(f) Convention relating to the Status of Refugees and its Protocol;

(g) Counter-Terrorism Implementation Task Force, *Basic Human Rights Reference Guide: Security Infrastructure* (New York, 2014);

(h) OHCHR, *Recommended Principles and Guidelines on Human Rights at International Borders* (Geneva, 2014);

(i) Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: implementation of General Assembly resolution 60/251 of 15 March 2006 entitled "Human Rights Council" (A/HRC/4/26);

(j) INTERPOL, I-24/7 secure global police communications system.

C. Enhancing dialogue, broadening understanding and developing a comprehensive approach to preventing the spread of terrorism

395. In paragraph 3 of resolution 1624 (2005), the Council calls upon all States to continue international efforts to enhance dialogue and broaden understanding among civilizations in an effort to prevent the indiscriminate targeting of different religions and cultures. Constructive dialogue between Governments and communities is a crucial factor in building community resilience, identifying and addressing grievances and working to prevent recruitment.[369] Enhancing dialogue and deepening the understanding of drivers of violent extremism can help States to develop comprehensive and coordinated approaches to preventing the spread of terrorism and violent extremism.[370] In paragraph 16 of resolution 2178 (2014), the Council encourages Member States to engage relevant local communities and non-governmental actors in developing strategies to counter the violent extremist narrative that can incite terrorist acts and address the conditions conducive to the spread of violent extremism, which can be conducive to terrorism. States should

[368] Resolution 1624 (2005), paras. 1 (c) and 4; and Universal Declaration of Human Rights, art. 14.
[369] Madrid Guiding Principles, guiding principle 2.
[370] Resolution 2129 (2013), para. 19.

consider devoting greater resources to supporting social services and funding relevant research in order to strengthen their understanding of the reasons why individuals become aspiring foreign terrorist fighters. In many cases, individualized intervention may be the only effective way to address radicalization to violence.[371]

396. In resolutions 2242 (2015) and 2395 (2017), the Council calls upon the Counter-Terrorism Committee Executive Directorate, within its existing mandate and in collaboration with the United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women), to conduct and gather gender-sensitive research and data collection on the drivers of radicalization for women and the impacts of counter-terrorism strategies on women's human rights and women's organization, in order to develop targeted and evidence-based policy and programming responses. In this regard, the State should ensure that outreach to civil society and key partners allows for the meaningful participation of women and women's groups as part of a whole-of-society and whole-of-government approach to developing national regional strategies to counter terrorism and violent extremism. Efforts to strengthen measures to prevent and counter violent extremism, as set forth in resolution 2178 (2014), can also support the implementation of resolution 1624 (2005).

397. The following issues should be considered:

(a) Has the State participated in international efforts to enhance dialogue and broaden understanding among civilizations in an effort to prevent the indiscriminate targeting of different religions and cultures?[372]

(b) Is the State engaged in national, subregional or regional counter-terrorism strategies that might address issues raised in resolution 1624 (2005)?[373]

(c) Has the State considered developing communications strategies in order to strengthen its understanding of the nature and appeal of violent extremist ideologies and promote non-violent alternative avenues for conflict prevention and resolution?[374]

(d) Has the State considered supporting relevant research in order to strengthen its understanding of the reasons why individuals become aspiring foreign terrorist fighters?[375]

(e) Does the State engage in, or encourage, community-awareness briefings, town halls, advisory committees and other platforms for communities to express grievances and discuss community concerns, involving both governmental and non-governmental actors?[376]

398. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principle 8;

(b) Addendum to the Madrid Guiding Principles, guiding principle 39;

---

[371] Madrid Guiding Principles, guiding principle 1.

[372] Counter-Terrorism Committee Executive Directorate, detailed implementation survey for resolution 1624 (2005), template 6.

[373] Resolution 1963 (2010), in which the Council encourages the Counter-Terrorism Committee Executive Directorate, in close cooperation with the Counter-Terrorism Implementation Task Force and its relevant working groups, to focus increased attention on resolution 1624 (2005) in its dialogue with Member States to develop, in accordance with their obligations under international law, strategies that include countering incitement of terrorist acts motivated by extremism and intolerance, and in facilitating technical assistance for its implementation, as called for in resolution 1624 (2005) and the United Nations Global Counter-Terrorism Strategy.

[374] S/2015/975, annex, para. 157 (a).

[375] Madrid Guiding Principles, guiding principle 1.

[376] Ibid., guiding principle 2.

(c) Hedayah, “Guidelines and good practices for developing national CVE strategies”.

D. Enhancing engagement with and empowering the media, civil and religious society, local communities, the business community, youth, families, women and other relevant non-governmental actors to counter incitement of terrorist acts, violent extremism and terrorist narratives

399. In resolution 1624 (2005), the Council stresses the importance of the role of the media, civil and religious society, the business community and educational institutions in efforts to enhance dialogue and broaden understanding, promoting tolerance and coexistence and fostering an environment that is not conducive to incitement of terrorism. In paragraph 16 of resolution 2178 (2014), the Council encourages Member States to engage relevant local communities and non-governmental actors, including by empowering youth, families, women, religious, cultural and education leaders and all other concerned groups of civil society, and to adopt tailored approaches to countering recruitment to violent extremism that can incite terrorist acts and promoting social inclusion and cohesion. Local communities can provide valuable insights into the factors that make individuals targets of incitement and recruitment to commit terrorist acts, and thus can play a key role in prevention.[377] To further this objective, States should work to create space for civil society and develop innovative mechanisms for dialogue between the Government and local communities, youth, families, women, religious, cultural and education leaders and other concerned groups.[378] In resolutions 2122 (2013) and 2242 (2015), the Council highlights the potential roles of women, underscoring the principles outlined in resolution 1325 (2000) and applying them to international counter-terrorism efforts, in particular those efforts to implement resolutions 1373 (2001), 1624 (2005) and 2178 (2014).

400. In paragraph 19 of resolution 2178 (2014), the Council emphasizes the importance of Member States’ efforts to develop non-violent alternative avenues for conflict prevention and resolution by affected individuals and local communities to decrease the risk of radicalization to terrorism, and of efforts to promote peaceful alternatives to violent narratives espoused by foreign terrorist fighters, and underscores the role that education can play in countering terrorist narratives.

401. In resolution 2354 (2017), the Council urges Member States to consider implementing the comprehensive international framework to counter terrorist narratives submitted by the Counter-Terrorism Committee to the Council in April 2017 (S/2017/375, annex), with recommended guidelines and good practices to effectively counter the ways in which ISIL (Da’esh), Al-Qaida and associated individuals, groups, undertakings and entities use their narratives to encourage, motivate and recruit others to commit terrorist acts. The comprehensive framework consists of three core elements: (a) legal and law enforcement measures in accordance with obligations under international law and consistent with United Nations resolutions; (b) public-private partnerships; and (c) counter-narratives. In resolution 2354 (2017), the Council emphasizes that, in developing and implementing counter-narratives and programmes, States should consider: (a) tailoring counter-narratives and programmes to the specific circumstances of different contexts at all levels; (b) engaging with a wide range of actors, including youth, families, women, religious, cultural and education leaders and other concerned groups of civil society; (c) supporting efforts aimed at raising public awareness regarding counter-terrorist narratives through education and the media,

[377] Madrid Guiding Principles, guiding principle 6.

[378] Ibid., guiding principle 2.

including through dedicated educational programmes to pre-empt youth acceptance of terrorist narratives; (d) aiming not only to rebut terrorists' messages, but also to amplify positive narratives and to provide credible alternatives and address issues of concern to vulnerable audiences who are subject to terrorist narratives; (e) taking into account the gender dimension and developing narratives that address the specific concerns and vulnerabilities of both men and women; and (f) supporting continued research into the drivers of terrorism and violent extremism. The Council reiterates that all measures taken by Member States to counter terrorism, including to counter terrorist narratives, must comply with their obligations under international law, including international human rights law, international refugee law and international humanitarian law.

402. In its resolution 2396 (2017), the Council recognizes that a comprehensive approach to the threat posed by foreign terrorist fighters requires addressing the conditions conducive to the spread of terrorism, including by preventing radicalization to terrorism; stemming recruitment; disrupting financial support to terrorists; countering incitement to commit terrorist acts; promoting political and religious tolerance, good governance, economic development, social cohesion and inclusiveness; ending and resolving armed conflicts; and facilitating investigation, prosecution, reintegration and rehabilitation.

403. In the same resolution, the Council notes with concern that terrorists craft distorted narratives to polarize communities, recruit supporters and foreign terrorist fighters, mobilize resources and garner support from sympathizers, in particular by exploiting ICT, including the Internet and social media. The Council stresses the need to effectively counter the ways in which ISIL (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities use their narratives to incite and recruit others to commit terrorist acts, and recalls, in that regard, its resolution 2354 (2017) and the comprehensive international framework to counter terrorist narratives.

404. Member States and the United Nations system are also urged to take measures, pursuant to international law, to address, in a balanced manner, all internal and external drivers of violent extremism that is conducive to terrorism, in accordance with the United Nations Global Counter-Terrorism Strategy. Member States are also called upon to develop and implement risk assessment tools to identify individuals who demonstrate signs of radicalization to violence and to develop intervention programmes, including with a gender perspective, in compliance with applicable international and domestic law and without resorting to profiling based on any discriminatory grounds prohibited by international law.

405. Member States bear the primary responsibility in these areas. However, the value of engagement with relevant local communities and non-governmental actors should also be acknowledged. States should consider supporting youth, families, women, religious, cultural and education leaders and other concerned civil society groups in their efforts.

406. The following issues should be considered:

(a) What measures has the State taken to counter incitement of terrorist acts motivated by extremism and intolerance, including with the participation of local communities, the private sector, civil society, the media and other relevant non-governmental actors, while safeguarding the rights to freedom of expression and association, maintaining the independence of civil society and human rights defenders and ensuring the right to personal security, in accordance with its obligations under international law?[379]

[379] Resolution 2178 (2014), para. 16; resolution 2354 (2017), preamble and para. 2 (f); and Madrid Guiding Principles, guiding principle 2.

(b) What measures has the State taken to promote greater inclusion of women in civil society to counter incitement of terrorist acts and violent extremism?[380]

(c) How has the State endeavoured to ensure that efforts to counter terrorism and violent extremism do no harm, in particular regarding women and youth?[381]

(d) What steps has the State taken to meaningfully engage youth in efforts to counter incitement of terrorist acts and violent extremism?[382]

(e) Has the State considered establishing partnerships with victims and victims' associations?[383]

(f) Is the State effectively collaborating with ICT industry actors in order to implement effective strategies to counter the threat of online radicalization?[384]

(g) Does the State delineate the respective roles of Governments and civil society actors in countering violent extremism?[385]

(h) Has the State developed programmes to strengthen the engagement of young people in countering violent extremism, such as youth-mentorship and skills-development programmes, community service projects, and enhanced educational opportunities that increase their sense of belonging?[386]

(i) Does the State engage in communication with families while ensuring that such interaction is voluntary and not imposed? Does the State provide support to services that engage with families, provided that such services are kept separate from security agencies?[387]

(j) Has the State considered the role of victims of terrorism in countering radicalization to violence, particularly in the form of efforts to counter terrorist narratives and online recruitment attempts?[388]

(k) Has the State engaged in efforts to counter terrorists' narratives, in accordance with the approach and guidelines set forth in resolutions 2354 (2017) and 2396 (2017) and related documents, such as the comprehensive international framework to counter terrorist narratives?

(l) Have efforts to counter terrorist narratives and/or offer positive/alternative narratives been undertaken in partnership with youth, families, women, religious, cultural and education leaders or other concerned groups of civil society?[389]

(m) Has the State developed clear goals and objectives for counter-narrative measures and programmes and shared those with all actors expected to play a role in implementing those measures and programmes? Does the State support efforts to evaluate the effectiveness of such measures and programmes?[390]

---

[380] Madrid Guiding Principles, guiding principle 8; and resolution 2354 (2017), preamble and para. 2 (f) and (k).

[381] Madrid Guiding Principles, guiding principles 8 and 9.

[382] Resolution 2178 (2014), para. 16; and Madrid Guiding Principles, guiding principle 9.

[383] Statement by the President of the Security Council of 11 May 2016 (S/PRST/2016/6); and Madrid Guiding Principles, guiding principle 6.

[384] S/2017/375, annex; and resolution 2354 (2017), paras. 1 and 2. See also Madrid Guiding Principles, guiding principle 26.

[385] Madrid Guiding Principles, guiding principle 7; and resolution 1624 (2005), para. 3.

[386] Resolution 2178 (2014), para. 16; resolution 2354 (2017), preamble and para. 2 (f) and (g); and Madrid Guiding Principles, guiding principles 2, 7 and 9.

[387] Resolution 2178 (2014), para. 16; resolution 2354 (2017), para. 2 (f); Madrid Guiding Principles, guiding principle 2; and S/2015/338, annex, para. 3.

[388] Madrid Guiding Principles, guiding principle 6.

[389] Resolution 2354 (2017), para. 2 (f).

[390] Ibid., para. 4 (g).

(n) What legal and law enforcement measures are used by the State to address the problem of terrorist narratives?[391]

(o) Has the State explored the development of public-private partnerships in order to strengthen its approach to countering terrorist narratives?[392]

(p) Does the State engage in voluntary cooperation with the private sector and civil society to develop and implement more effective means to counter the use of the Internet for terrorist purposes, including by developing counter-terrorist narratives and through innovative technological solutions?

(q) Does the State engage, where appropriate, with religious authorities, community leaders and other civil society actors, including women's civil society organizations, who have relevant expertise in crafting and delivering effective counter-narratives, in countering narratives used by terrorists, including foreign terrorist fighters and their supporters?

(r) Does the State encourage the leadership and participation of women in the pursuit of effective counter-narrative strategies and efforts to counter violent extremism that leads to terrorism and to address the conditions conducive to terrorism?

(s) Does the State encourage the leadership and participation of youth in the pursuit of effective counter-narrative strategies and efforts to counter violent extremism that leads to terrorism and to address the conditions conducive to terrorism?

(t) Does the State ensure that all actors expected to play a role in implementing counter-narrative measures and programmes have the necessary resources, training and guidance to do so effectively and in a human rights compliant and gender- and age-sensitive manner?

(u) How does the State seek to ensure that its initiatives in the area of countering terrorist narratives comply with its obligations under international law, including international human rights law, international refugee law and international humanitarian law?[393]

(v) Are counter-narrative measures and programmes tailored to the specific circumstance of different contexts at all levels?[394] Do they include gender-specific programming?

(w) Has the State sought technical assistance in this area from international or regional organizations, such as the United Nations Educational, Scientific and Cultural Organization, the United Nations Development Programme or other member entities of the United Nations Global Counter-Terrorism Coordination Compact Task Force (formerly known as the Counter-Terrorism Implementation Task Force), Member States, international civil society organizations or other relevant assistance provider?

407. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principle 8;

(b) Addendum to the Madrid Guiding Principles, guiding principle 39;

[391] S/2017/375, annex; and resolution 2354 (2017), paras. 1 and 2.
[392] Madrid Guiding Principles, guiding principle 26; and resolution 2354 (2017).
[393] Resolution 2354 (2017), preamble and para. 2 (e).
[394] Resolution 2354 (2017), para. 2 (d).

(c) Strategic Policy and Development Section of the Police Division, Office of Rule of Law and Security Institutions, Department of Peacekeeping Operations, United Nations Police Gender Toolkit, 2015;

(d) European Commission, Radicalization Awareness Network declaration of good practices for engagement with foreign fighters for prevention, outreach, rehabilitation and reintegration;

(e) European Commission, Radicalization Awareness Network, *Collection of Approaches and Practices: Preventing Radicalisation to Terrorism and Violent Extremism* (2019), practice 2.5.31, "Holding difficult conversations";

(f) Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief;

(g) OSCE, Guidebooks on the role of civil society in preventing and countering violent extremism and radicalization that lead to terrorism, focused on various geographic regions (forthcoming);

(h) Henry Tuck and Tanya Silverman, *The Counter-Narrative Handbook* (Institute for Strategic Dialogue, June 2016), and Louis Reynolds and Henry Tuck, *The Counter-Narrative Monitoring & Evaluation Handbook* (Institute for Strategic Dialogue, November 2016).

E. Preventing the subversion of educational, cultural and religious institutions by terrorists and their supporters

408. In resolution 1624 (2005), the Council calls upon all States to take all measures as may be necessary and appropriate and in accordance with their obligations under international law to prevent the subversion of educational, cultural and religious institutions by terrorists and their supporters.[395]

409. States are also obliged under international human rights law to prohibit the advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. Local communities are often best placed to engage with religious institutions in order to prevent their subversion by terrorists and their supporters.

410. Consideration should also be given to promoting greater engagement of women in this effort.[396]

411. The following issues should be considered:

(a) What measures have been taken by the State to prevent the subversion of educational, cultural and religious institutions by terrorists and their supporters?[397]

(b) Has the State considered engaging religious leaders to provide a platform for intrafaith and interfaith dialogue and discussions through which to promote tolerance and understanding among communities?[398]

(c) Has the State developed any specific measure aimed at supervising the nomination and training of religious leaders?[399]

[395] Counter-Terrorism Committee Executive Directorate, detailed implementation survey for resolution 1624 (2005), template 11.
[396] S/2016/50, annex, para. 63.
[397] Madrid Guiding Principles, guiding principle 5.
[398] S/2016/50, annex, para. 46.
[399] Ibid., para. 56.

(d) Does the State supervise, through appropriate channels, the drafting of religious and non-religious school curriculums?[400]

(e) Has the State considered devoting resources to educational programmes that develop critical thinking and build awareness and understanding of different cultures?[401]

(f) Has the State developed any programme aimed at strengthening the teaching of religious tolerance in schools at all levels?[402]

(g) How has the State endeavoured to ensure that its efforts in this field are consistent with its obligations under international law, including respect for the right to freedom of thought, conscience and religion, and freedom to manifest one's religion or beliefs, subject only to certain permissible limitations as provided for under international law?[403]

412. The following international instruments, standards and good practices provide guidance in this area:

(a) Universal Declaration of Human Rights, article 18; International Covenant on Civil and Political Rights, articles 18 and 20;

(b) Human Rights Committee, general comment No. 22 (1993) on freedom of thought, conscience and religion (article 18 of the International Covenant on Civil and Political Rights);

(c) Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief;

(d) Reports of the Special Rapporteur on freedom of religion or belief.

F. Risk assessment and intervention programmes

413. In its resolution 2396 (2017), the Council calls upon Member States to develop and implement risk assessment tools to identify individuals who demonstrate signs of radicalization to violence and to develop intervention programmes, including with a gender perspective, in compliance with applicable international and domestic law and without resorting to profiling based on any discriminatory grounds prohibited by international law.

414. The following issues should be considered:

(a) Has the State developed and implemented risk assessment tools to identify individuals who demonstrate signs of radicalization to violence, including with a gender perspective,[404] without resorting to profiling based on any discriminatory grounds prohibited by international law?

(b) Has the State developed intervention programmes, including with a gender perspective, as appropriate, to prevent individuals from committing acts of terrorism, in compliance with applicable international and domestic law and without resorting to profiling based on any discriminatory grounds prohibited by international law?

(c) Has the State developed or supported mechanisms to evaluate risk assessment tools and intervention programmes?

[400] Ibid., para. 58.
[401] S/PRST/2016/6.
[402] Ibid.
[403] Resolution 1624 (2005), para. 4.
[404] Resolution 2396 (2017), para. 38.

(d) Does the State ensure the continuous training, development and validation of professionals involved in risk assessment?

(e) Has the State put in place independent oversight mechanisms and ensured accountability of professionals involved in risk assessments?

415. The following international instruments, standards and good practices provide guidance in this area:

(a) Addendum to the Madrid Guiding Principles, guiding principle 40;

(b) OHCHR, Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, 2012;

(c) OSCE, *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach* (Vienna, February 2014);

(d) Council of Europe Convention on the Prevention of Terrorism, article 5 (the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has cited article 5 as a good practice in criminalizing terrorists).

G. International cooperation

416. In paragraph 18 of its resolution 2178 (2014), the Council notes the importance of international cooperation in the context of countering violent extremism and calls upon Member States to cooperate and consistently support other States' efforts to counter violent extremism, which can be conducive to terrorism, including through capacity-building, the coordination of plans and efforts and the sharing of lessons learned.

417. The following issues should be considered:

(a) Has the State considered strengthening international legal cooperation regarding content intended to incite terrorist acts or radicalize individuals to violence, considering that Internet servers might be hosted abroad?

(b) What measures of assistance has the State afforded other States in connection with investigations or proceedings relating to incitement to commit terrorist acts?[405]

(c) Does the State facilitate cooperation across key stakeholder agencies and ministries, as well as experts and practitioners, to foster regional approaches to countering incitement and violent extremism?

418. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles, guiding principle 24;

(b) Addendum to the Madrid Guiding Principles, guiding principle 49;

(c) Council of Europe Convention on the Prevention of Terrorism, article 4.

[405] Madrid Guiding Principles, guiding principle 33.

H. Complying with international human rights, refugee and humanitarian law

419. In paragraph 4 of resolution 1624 (2005), the Council stresses that States must ensure that any measures taken to implement paragraphs 1, 2 and 3 of the resolution comply with all their obligations under international law, in particular international human rights, refugee and humanitarian law. Among other measures, States are under an obligation to safeguard the ability of non-governmental actors to operate in a secure environment with full respect for the peaceful exercise of human rights and fundamental freedom, including the freedoms of thought, conscience, expression, religion, peaceful assembly and association.[406]

420. The State must ensure that any measures taken to prevent and counter incitement and violent extremism comply with all its obligations under international law, in particular international human rights law, international refugee law and international humanitarian law,[407] bearing in mind that shortcomings in States' efforts in this regard may be exploited by terrorists for recruitment purposes.[408]

421. Women and children associated with foreign terrorist fighters returning and relocating from conflict may require special focus and assistance, as they may have served in many different roles, including as supporters, facilitators or perpetrators of terrorists acts, and may be victims of terrorism. States should pay particular attention to ensuring that their domestic legislation respects international law with regard to women and children and should take into account the best interests of the child as a primary consideration.

422. The following issues should be considered:

(a) What laws, policies and measures has the State put in place to protect the right to freedom of expression and opinion while countering terrorist incitement,[409] both offline and online?

(b) What laws, policies and measures has the State put in place to protect the right to freedom of religion or belief while countering terrorist incitement?[410]

(c) What laws, policies and measures has the State put in place to protect the right to freedom of peaceful assembly and association while countering terrorist incitement?[411]

(d) What are examples of challenges encountered by the State in its efforts to ensure that any measures taken to implement paragraphs 1, 2 and 3 of resolution 1624 (2005) comply with all its obligations under international law, in particular international human rights, refugee and humanitarian law?[412]

(e) Are there ongoing efforts to engage with civil society, traditional and faith leaders, women and youth groups, to help to ensure the protection of their rights in the context of efforts to counter incitement and violent extremism?[413]

423. The following issue should be considered with respect to international humanitarian law: Does the State ensure that all measures taken to counter terrorism,

[406] Ibid., guiding principle 10.
[407] Human Rights Council resolution 30/15.
[408] S/2016/49, annex, para. 397.
[409] Resolution 1624 (2005), preamble.
[410] Ibid.
[411] Ibid., preamble and para. 4.
[412] Counter-Terrorism Committee Executive Directorate, detailed implementation survey for resolution 1624 (2005), template 10.
[413] Resolution 2178 (2014); and Madrid Guiding Principles, guiding principle 7.

including measures taken to counter the financing of terrorism, comply with its obligations under international law, including international humanitarian law, international human rights law and international refugee law?[414] Does the State, when designing and applying measures to counter the financing of terrorism, take into account the potential effect of those measures on exclusively humanitarian activities, including medical activities, that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law?[415]

424. The following issues should be considered with respect to the rights of the child: Has the State put in place special safeguards and legal protections to ensure that appropriate action is taken in cases involving children, in full compliance with their obligations under international law, ensuring that the competent authorities:

(a) Fully respect and promote the rights of the child, taking into account the best interests of the child as a primary consideration;

(b) Take into consideration the age of the child and the many roles in which children associated with foreign terrorist fighters may have served, while recognizing that such children may be victims of terrorism;

(c) Consider the impact of terrorism on children and children's rights, especially with regard to issues relating to the families of returning and relocating foreign terrorist fighters;

(d) Assess each child individually and without prejudice, and take his or her rights and needs into account, while also considering the circumstances relating to the case and proceeding with any further criminal or security-related actions;

(e) Are provided with appropriate scope for discretion at all stages of proceedings and have at their disposal a variety of alternatives to judicial proceedings and sentencing, including (if appropriate) age-sensitive child protection measures;

(f) Are provided with clear guidelines with respect to whether, or under what conditions, they should keep a child in detention and in which cases diversion is possible, subject to regulation and review, in accordance with international law and domestic standards, and bearing in mind that, in cases involving children, detention should be used as a measure of last resort;

(g) Act in accordance with the guidelines regulating pretrial detention and the utilization of other measures of restraint, as provided for in their criminal legislation and defined in compliance with international law?[416]

425. The following international instruments, standards and good practices provide guidance in this area:

(a) Madrid Guiding Principles;

(b) Addendum to the Madrid Guiding Principles, guiding principles 41 and 42;

(c) Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights;

(d) Johannesburg Principles on National Security, Freedom of Expression and Access to Information;

(e) Human Rights Council resolution 32/13 on the promotion, protection and enjoyment of human rights on the Internet.

---

[414] Resolution 2462 (2019), para. 6.

[415] Ibid., para. 24.

[416] Addendum to the Madrid Guiding Principles, guiding principle 42.