

**Security Council**

Distr.: General
27 December 2022

Original: English

**Letter dated 22 December 2022 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 herewith to the Security Council the Delhi Declaration outcome document of the special meeting of the Counter-Terrorism Committee on countering the use of new and emerging technologies for terrorist purposes.

The special meeting was held on 28 and 29 October 2022 in Mumbai and New Delhi, India, and was attended by the wider membership of the United Nations, international and regional organizations, United Nations bodies, the private sector and members of civil society organizations, academia and the media.

The Committee should be grateful if the present letter and its attachment were brought to the attention of the members of the Security Council and issued as a document of the Council, as well as transmitted to the President of the General Assembly.

(Signed) Ruchira **Kamboj**
Chair

Security Council Committee established pursuant to resolution
[1373 \(2001\)](#) concerning counter-terrorism



Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes

New Delhi, India,
29 October 2022

The Counter-Terrorism Committee,

1. *Reaffirms* that terrorism in all forms and manifestations constitutes one of the most serious threats to international peace and security, and that any acts of terrorism are criminal and unjustifiable regardless of their motivations, whenever, wherever, and by whomsoever committed, and remains determined to contribute further to enhancing the effectiveness of the overall effort to fight this scourge on a global level,
2. *Emphasizes* that the threat of terrorism is continuing, affecting a greater number of Member States across most regions, which exacerbates conflicts in affected regions, and contributes to undermining affected States, specifically their security, stability, governance, social and economic development,
3. *Reaffirms* that terrorism should not be associated with any religion, nationality, civilization or ethnic group,
4. *Expresses* deep concern that terrorism, in all its forms and manifestations, has become more diffuse, with an increase, in various regions of the world, notably aided by terrorists' adaptation to, and the use of new and emerging technologies, for terrorist purposes, while recognizing that innovations in technology may offer significant counter-terrorism opportunities,
5. *Notes* with concern the increased use, in a globalized society, by terrorists and their supporters of Internet and other information and communications technologies, including social media platforms, for terrorist purposes, such as for recruitment and incitement to commit terrorist acts, as well as for the financing, planning, and preparation of their activities,
6. *Recognizes* that innovations in financial technologies, products and services, such as virtual assets and new financial instruments, including, but not limited to, crowdfunding platforms, may offer economic opportunities but also present a risk of being misused, including for terrorist-financing,
7. *Notes* with additional concern the increasing global misuse of unmanned aerial systems (UAS) by terrorists to conduct attacks against, and incursions into critical infrastructure and soft targets or public places, and to traffic drugs and arms,
8. *Acknowledges* the need to balance fostering innovation and preventing and countering the use of new and emerging technologies, as their application expands, for terrorist purposes, and emphasizes the need to preserve global connectivity and the free and secure flow of information facilitating economic development, communication, participation and access to information,
9. *Urges* all Member States to take urgent action to prevent and counter terrorism in all its forms and manifestations through the full and effective implementation of Security Council resolutions [1373 \(2001\)](#), [1624 \(2005\)](#), [2178 \(2014\)](#), [2396 \(2017\)](#), [2617 \(2021\)](#) and other relevant international instruments relating to terrorism, consistent with their obligations under international law,
10. *Noting* the importance of Member States integrating gender as a cross-cutting issue into their counter-terrorism strategies and activities,
11. *Calls on* Member States to fulfil their obligations enshrined in relevant international counter terrorism conventions and protocols to which they are a party,

and recognizes Member States' continuing efforts towards the Comprehensive Convention on International Terrorism,

12. *Underscores* the obligation of Member States to prevent and suppress the financing of terrorist acts and to 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, consistent with international law, and eliminating the supply of weapons to terrorists,

13. *Underlines* that terrorists' opportunity to access safe havens continues to be a significant concern and that all Member States must cooperate fully in the fight against terrorism in order to identify safe havens, deny terrorists' access to them and bring to justice, in accordance with domestic and international laws, any person who supports, facilitates, participates or attempts to participate in the financing, planning, preparation or commission of terrorist acts, including by providing safe havens,

14. *Reaffirms* that Member States must ensure that any measures taken to counter terrorism, including the use of new and emerging technologies for terrorist purposes respect the Charter of the United Nations and comply with their obligations under international law, including international human rights law, international humanitarian law and international refugee law, as applicable,

15. *Emphasizes* the need for Member States to act cooperatively to prevent and counter the use of new information and communications technologies, and other emerging technologies, for terrorist purposes, including recruitment and incitement to commit terrorist acts, as well as the financing, planning and preparation of their activities and stresses the importance of cooperation with civil society and the private sector in this endeavor,

16. *Notes* the importance of continuing discussions on the challenges posed by emerging technologies being used for terrorist purposes in other relevant international forums including the G20, and also notes the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online,

17. *Further emphasizes* the need for Member States to continue voluntary cooperation with the private sector and civil society, to develop and implement more effective means to counter the use of new and emerging technologies, including the Internet, for terrorist purposes,

18. *Stresses* the need to effectively counter the ways that the ISIL also known as Daesh, Al-Qaida, their affiliates and associated individuals, groups, undertakings, and entities use their narratives to incite and recruit others to commit terrorist acts,

19. *Recalls* the Counter-Terrorism Committee's Comprehensive International Framework to Counter Terrorist Narratives ([S/2017/375](#)) and Security Council resolution [2354 \(2017\)](#), which request the Committee to continue to identify and compile existing good practices in countering terrorist narratives; emphasizes the need for Member States to develop counter-terrorist narratives and innovative technological solutions, all while respecting international law,

20. *Recognizes* the efforts of the United Nations-affiliated Tech Against Terrorism initiative to foster collaboration with representatives of the technology industry, including smaller technology companies, civil society, academia, and Government, to disrupt terrorists' ability to use the Internet in furtherance of terrorist purposes, while also respecting human rights and fundamental freedoms; takes note of the industry-led Global Internet Forum to Counter Terrorism (GIFCT) initiatives; and reiterates its call for the GIFCT to continue to increase engagement with Governments and technology companies globally,

21. *Recalls* that Member States should consider and assess risks associated with specific products and payment methods, including value stored and prepaid cards, virtual assets and new financial instruments, including, but not limited to, crowdfunding platforms, and implement risk-based anti-money-laundering (AML) and counter-terrorist financing (CFT) regulations, monitoring, and supervision to providers of relevant services, and acknowledges the important work and the essential role of the Financial Action Task Force (FATF) in this regard,
22. *Reiterates* its call for Member States to enhance the traceability and transparency of financial transactions, consistent with international law including international human rights law and humanitarian law, via, inter alia, fully exploiting the use of new and emerging financial and regulatory technologies to bolster responsible financial inclusion for legitimate users, and to contribute to the effective implementation of AML/CFT measures,
23. *Recognizes* the ongoing work of the FATF concerning virtual assets and virtual assets service providers (VASPs), as well as the opportunities that technology can offer to improve AML/CFT efforts, and calls upon the FATF to undertake further work on identifying how to improve global implementation of counter-terrorist financing measures,
24. *Calls on* Member States to further enhance the specialized expertise and capacity of the authorities engaged in handling increasingly complex cases on terrorism financing that involve advanced investigation techniques and complex international cooperation mechanisms in order to keep pace with the rapid evolution in financial tools and terrorism-financing methods,
25. *Encourages* the competent national authorities, in particular financial intelligence units and intelligence services, to continue to establish effective partnerships with the private sector, including financial institutions, the financial technology industry and Internet and social media companies, with regard to the evolution of trends, sources, and methods of the financing of terrorism,
26. *Strongly condemns* the continued flow of weapons, military equipment, UAS and their components, and improvised explosive device (IED) component to and between ISIL/Da'esh, Al-Qaida, their affiliates and associated individuals, groups, undertakings, and entities, and other terrorist groups, and illegal armed groups and criminals, and encourages Member States to prevent and disrupt procurement networks for such weapons, systems, UAS and components to ISIL/Da'esh, Al-Qaida, their affiliates and associated individuals, groups, undertakings, and entities, and other terrorist groups,
27. *Reiterates* its call for Member States to address, consistent with international law, the threat posed by the use of UAS for terrorist purposes, acknowledges the need to balance fostering innovation and preventing the use of UAS for terrorist purposes as its applications expand and takes note of international efforts that contribute to raising awareness of and preparedness for said use as the technology becomes more accessible and broadly used across the public and private sectors, including the publication entitled "The Protection of critical infrastructure against terrorist attacks: Compendium of good practices", developed jointly by the Counter-Terrorism Committee Executive Directorate (CTED), the United Nations Office of Counter-Terrorism (UNOCT), and the International Criminal Police organization (INTERPOL); and the Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems published by the Global Counterterrorism Forum (GCTF),
28. *Further calls on* Member States to develop a comprehensive understanding of the risks posed by terrorist use of UAS and of specific terrorist groups' systems for

acquiring UAS and their components, and possible links to other such systems; develop further measures to deter, detect and disrupt terrorist acquisition and use of UAS; engage in partnerships with the private sector and manufacturers; and ensure that the use of UAS for law enforcement and border-management purposes is exercised in compliance with international law, including international human rights law, international humanitarian law and international refugee law, as applicable,

29. *Notes* the “Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons” published by CTED, the United Nations Counter-Terrorism Centre (UNCCT), and the United Nations Institute for Disarmament Research (UNIDIR) within the framework of the United Nations Global Counter-Terrorism Coordination Compact Working Group on Border Management and Law Enforcement relating to Counter-Terrorism, and in particular its submodule on preventing terrorists from acquiring UAS and their components,

30. *Decides* to work on recommendations on the three themes of the CTC special meeting, namely “Countering Terrorist Exploitation of ICT and Emerging Technologies”, “Threats and opportunities related to new payment technologies and fundraising methods” and “Threats posed by misuse of unmanned aerial systems (UAS) by terrorists” after the conclusion of the Special Meeting,

31. *Resolves* to continue to assist Member States, with the support of CTED, to achieve full implementation of all relevant Security Council resolutions that pertain to countering the use of new and emerging technologies for terrorist purposes, while respecting human rights and fundamental freedoms,

32. *Expresses* intention to develop, with the support of CTED, set of non-binding guiding principles, taking into consideration the above, with a view to assisting Member States to counter the threat posed by the use of new and emerging technologies for terrorist purposes, including by compiling good practices on the opportunities offered by the same set of technologies to counter the threat, consistent with international human rights and international humanitarian law,

33. *Encourages* CTED to deepen its engagement and cooperation with civil society, including women and women’s organizations, relevant private-sector entities, and other stakeholders, as appropriate, as well as in the identification of trends, emerging issues and developments, with the support of members of the CTED Global Research Network (GRN), on areas pertaining to the threat posed by the use of new and emerging technologies for terrorist purposes,

34. *Further encourages* CTED to consider building on, strategic and voluntary public-private partnerships to ensure the timely exchange of information, support the conducting of threat analysis, the collation of good practices and, as appropriate, the development of operational support in countering the threat posed by the use of new and emerging technologies for terrorist purposes, while also harnessing the expertise present within the GRN,

35. *Welcomes* the efforts of CTED to facilitate, in close cooperation with UNOCT, the relevant United Nations Global Counter-Terrorism Coordination Compact entities, and other international specialized agencies, the delivery of technical assistance to Member States, upon request, mindful of the opportunities offered by new and emerging technologies to counter the terrorist threat, and requests CTED to produce a gap analysis, for consideration of the committee, on the capacities of Member States to counter the use of new and emerging technologies for terrorist purposes.