United Nations S/2025/22

Security Council

Distr.: General
10 January 2025

Original: English

Letter dated 9 January 2025 from the President of the Security Council acting in the absence of a 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 refer to the non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes (see annex), to be known and referred to as the "Algeria Guiding Principles", prepared in accordance with the Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes, in which the Committee decided to develop a set of non-binding guiding principles to assist Member States in countering the threat posed by the use of new and emerging technologies for terrorist purposes.

I wish to request that the present letter and its annex be issued as a Security Council document.

(*Signed*) Amar **Bendjama**
President of the Security Council acting in the absence of a Chair
of the Security Council Committee established pursuant to
resolution 1373 (2001) concerning counter-terrorism

Annex

Non-binding guiding principles for Member States on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes[1]

1. New and emerging technologies provide far-reaching potential benefits in multiple domains, including in public health, border control, law enforcement, transportation, humanitarian assistance and communication systems.

2. New and emerging technologies, while providing many benefits to society, are being used for terrorist purposes by ISIL (Da'esh), Al-Qaida, their affiliated groups, other terrorist organizations and their supporters. Member States already face a significant and growing threat from the exploitation of new and emerging technologies to facilitate a wide range of terrorist activities.

3. Mindful of the increasing threat posed by the misuse of new and emerging technologies, as well as the many beneficial uses of technologies for countering terrorism, the Counter-Terrorism Committee held a special meeting on countering the use of new and emerging technologies for terrorist purposes in India and adopted the Delhi Declaration on 29 October 2022.

4. The Counter-Terrorism Committee also expressed its intention to develop, with the support of the Counter-Terrorism Committee Executive Directorate, a set of non-binding guiding principles with a view to assisting Member States in countering 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. To facilitate the development of the guiding principles, the Executive Directorate, on behalf of the Committee, undertook a comprehensive consultative process on each of the three themes with relevant experts from United Nations agencies and international and regional organization partners, as well as a range of relevant stakeholders from the Executive Directorate's Global Counter-Terrorism Research Network, including the private sector, academia and civil society.

5. The Security Council has reaffirmed that Member States must ensure that any measures taken to combat the threat posed by new and emerging technologies used for terrorist purposes comply with all their obligations under international law, in particular international human rights law, international refugee law and international humanitarian law; underscored that effective counter-terrorism measures and respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing, and are an essential part of a successful counter-terrorism effort; and noted the importance of integrating gender as a cross-cutting issue, in line with Council resolution 2617 (2021).

6. The present set of non-binding guiding principles have been developed by the Counter-Terrorism Committee and are an effort to assist Member States in countering the use of new and emerging technologies for terrorist purposes in a manner consistent with international law.

[1] The purpose and focus of these non-binding guiding principles is to assist Member States in enhancing national measures and strengthening international cooperation; the non-binding guiding principles do not purport to impose any legal obligations upon States.

7. The following guiding principles are intended to complement other materials in order to guide Member States and the work of the Counter-Terrorism Committee and the Counter-Terrorism Committee Executive Directorate to support States in their implementation of Security Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2370 (2017), 2396 (2017), 2462 (2019), 2617 (2021) and other relevant Council documents on counter-terrorism.[2] Many of the guiding principles set forth in the present document build upon the work and recommended good practices of the Security Council and General Assembly, United Nations partner organizations and other key stakeholders, such as the Financial Action Task Force.

Threats posed by the use of new and emerging financial technologies for terrorist purposes

8. As recognized by the Security Council, innovations in financial technologies may offer significant economic opportunities.[3] They may also present a risk of being misused, including for terrorist purposes.[4] The growing scale of the misuse has since been highlighted in several reports of the United Nations and the Financial Action Task Force and Financial Action Task Force-style regional bodies, as well as by members of the Executive Directorate's Global Counter-Terrorism Research Network and private sector partners.[5]

9. The scale and types of abuses vary considerably depending on regional and economic context, available means, and the targets set by terrorists in terms of their financing sources and methods. An increasingly popular trend in terrorist financing is

[2] These include the guiding principles on foreign terrorist fighters (S/2015/939); the addendum to the guiding principles on foreign terrorist fighters (2018) (S/2018/1177); the technical guide to the implementation of Security Council resolution 1373 (2001) and other resolutions (S/2019/998); the framework document for Counter-Terrorism Committee visits to Member States (S/2020/731); and the global survey of the implementation of resolution 1373 (2001) by Member States, issued in 2009, 2011, 2016 and 2021 (S/2009/620, S/2011/463, S/2016/49 and S/2021/972).

[3] Security Council resolution 2462 (2019), tenth preambular paragraph; see also Financial Action Task Force, *Opportunities and Challenges of New Technologies for AML/CFT* (Paris, 2021), available at https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html.

[4] Security Council resolution 2462 (2019), tenth preambular paragraph; also reiterated in resolution 2617 (2021), twenty-fifth preambular paragraph.

[5] For further details, see the eighteenth 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/2024/117), para. 14; the thirty-fourth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2024/556), paras. 94–97; Counter-Terrorism Committee Executive Directorate, Insight Briefing on Latest trends in the use of cryptocurrency by terrorist groups affiliated with Da'esh (ISIL)/Al-Qaida and their supporters, 4 March 2024 (see https://www.un.org/securitycouncil/ctc/news/cted-hosts-insight-briefing-%E2%80%9Clatest-trends-use-cryptocurrency-terrorist-groups-and-their); Financial Action Task Force, "Public statement on the financing of ISIL, Al Qaeda and affiliates", 21 October 2021, and subsequent non-public updates; and Asia/Pacific Group on Money Laundering, *APG Yearly Typologies Report 2021* (Sydney, 2021), available at www.apgml.org/includes/handlers/get-document.ashx?d=6bfd011b-8edd-40f4-93e4-f219e1c6d73e. See also e.g. *Elliptic, Preventing Financial Crime in Cryptoassets: Typologies Report 2022*, available at www.elliptic.co/resources/typologies-report-2022; TRM, *Illicit Crypto Ecosystem Report* (2023), available at www.trmlabs.com/illicit-crypto-ecosystem-report-2023; TRM, "Terrorist financing: six crypto-related trends to watch in 2023", 16 February 2023, available at https://www.trmlabs.com/post/terrorist-financing-six-crypto-related-trends-to-watch-in-2023; and TRM, "TRM finds mounting evidence of crypto use by ISIS and its supporters in Asia", 21 July 2023, available at https://www.trmlabs.com/post/trm-finds-mounting-evidence-of-crypto-use-by-isis-and-its-supporters-in-asia.

the mixed use of old and new ways to raise and move funds,[6] which essentially combines the challenges and complexities related to each method, from detecting physical cross-border transportation of cash to tracing intricate virtual transactions. States should therefore take a comprehensive and risk-based approach to countering the financing of terrorism (CFT), so that they do not neglect safeguards with regard to the methods and channels that are being exploited by terrorists. As such, a risk-based, current and efficient anti-money-laundering and countering the financing of terrorism (AML/CFT) framework, in line with international law, is essential to mitigate a plethora of terrorist financing vulnerabilities.

10. Examples of methods to raise funds for terrorist purposes through the use of new and emerging technologies include abuse of social networking services (used to solicit donations through traditional payment methods), content hosting services, online merchandise sales, and crowdfunding platforms.[7] In its most recent report, the Financial Action Task Force identified donation-based crowdfunding as most likely to be exploited for terrorist financing purposes of all the different forms of crowdfunding.[8] The four main typologies of crowdfunding abuse for terrorist financing purposes identified in the report are: abuse of humanitarian, charitable or non-profit causes; use of dedicated crowdfunding platforms or websites; use of social media platforms and messaging apps; and the interaction of crowdfunding with virtual assets. Yet, the regulatory oversight of the crowdfunding industry globally is still fragmented, including in relation to them being subject to AML/CFT rules.[9] Despite repeated instances of the use of social media and crowdfunding platforms by terrorists for financial activities, some platforms or chat applications face challenges in adapting self-monitoring and content moderation systems to address terrorist financing that may be occurring through their platforms.[10] There are also other fundraising opportunities that can be facilitated by online technologies and abused for terrorist purposes, such as the “super chat” feature or brands advertising and offering monetization alongside terrorist content, as trends and tactics continue to evolve.

11. Researchers, national authorities and multilateral policymakers indicate that, although cash and hawala-type systems remain the prevalent methods used to move money for terrorist purposes, accounting for most terrorist financing-related transfers, there is also an increase in their use in combination with the new technologies and payment methods. Mobile payment systems, virtual assets, and online exchanges and wallets have been abused for terrorist purposes, and such misuse is expected to become even more pervasive and significant.[11] The often complex money trail of these methods poses challenges for financial investigators, as well as for financial institutions when they interact. Some virtual assets can enable pseudonymous cross-

[6] This was also a prominent takeaway from the latest Financial Action Task Force joint expert meeting and the joint Financial Action Task Force/United Nations Office on Drugs and Crime workshop on terrorist financing through hawala and similar services (New Delhi, April 2023).

[7] S/2024/556, para. 94; see reference sources cited at www.un.org/securitycouncil/ctc/news/cted%E2%80%99s-tech-sessions-highlights-%E2%80%9Cthreats-and-opportunities-related-new-payment-technologies-0.

[8] Financial Action Task Force, *Crowdfunding for Terrorism Financing* (Paris, 2023), para. 38, available at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf.

[9] Ibid., paras. 27, 28 and 30. In the report, it is noted that only four jurisdictions in the Financial Action Task Force global network regulate both investment and donation-based crowdfunding in the context of their AML/CFT frameworks.

[10] For example, under the European Union Digital Services Act, large platforms are required to conduct their own risk assessment and remove illegal content upon notification from authorities, but there is no explicit reference to terrorist financing as a form of illegal content. As highlighted at the above-mentioned expert meetings, GoFundMe is currently the only crowdfunding platform that has specific provisions on terrorist financing in its terms of reference.

[11] S/2024/556, para. 95.

border peer-to-peer fund transfers,[12] which can occur without the involvement of a virtual asset service provider. These risks are compounded by persisting gaps in the implementation by countries of the Financial Action Task Force standards for virtual assets and virtual asset service providers, most notably recommendation 15 and the corresponding interpretive note. Decentralized finance and unhosted wallets, although a subset of the overall virtual asset ecosystem, pose terrorist financing and other financial crime risks. Some jurisdictions reported challenges in mitigating these risks.

12. The Security Council has called upon all Member States to assess and address potential risks associated with virtual assets and, as appropriate, the risks of new financial instruments, including but not limited to crowdfunding platforms, that may be abused for the purpose of terrorist financing and to take steps to ensure that providers of such assets are subject to AML/CFT obligations.[13]

13. The Security Council has also strongly urged all States to implement the comprehensive international standards embodied in the Financial Action Task Force revised Forty Recommendations on Combating Money Laundering and the Financing of Terrorism and Proliferation.[14] Recommendation 15 on new technologies (as revised in 2018 and supplemented with an interpretive note in 2019) indicates that countries and financial institutions should identify and assess the money-laundering or terrorist financing risks that may arise in relation to: (a) the development of new products and new business practices, including new delivery mechanisms; and (b) the use of new or developing technologies for both new and pre-existing products. To manage and mitigate the risks emerging from virtual assets,[15] countries should take steps to ensure that virtual asset service providers are regulated for AML/CFT purposes and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the Financial Action Task Force recommendations, or are otherwise prohibited from operating in the country.[16] In February 2023, the Financial Action Task Force adopted a road map to improve the implementation of recommendation 15. However, according to the Financial Action Task Force analysis, as of June 2024, many jurisdictions have made insufficient

[12] On the increased use of anonymity-enhancing cryptocurrencies (also called privacy coins) by ISIL and its affiliates, particularly Monero, a cryptocurrency that uses cryptographic technologies designed to obfuscate transaction details, see ibid., paras. 96 and 97.

[13] Resolution 2462 (2019), para. 20 (d).

[14] Ibid., para. 4.

[15] For more information, see Financial Action Task Force, Focus on Virtual Assets, available at https://www.fatf-gafi.org/en/topics/virtual-assets.html.

[16] For further details, see Financial Action Task Force, “Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers”, June 2024, pp. 4 and 5, available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html; and Financial Action Task Force, *Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers* (Paris, 2021), paras. 31–43.

progress in implementing the fundamental requirements of the Task Force on virtual assets and virtual asset service providers.[17]

14. Furthermore, the Security Council has called for the full use of new and emerging financial and regulatory technologies to bolster financial inclusion and to contribute to the effective implementation of AML/CFT measures, in compliance with international law. Indeed, and as highlighted by the work of the Financial Action Task Force, new technologies also have the potential to make AML/CFT measures in both the public and private sectors faster, cheaper, more transparent and more inclusive, while maintaining their safety and security.[18] When used responsibly and proportionally, technology can facilitate data collection, processing and analysis and help actors to identify and manage terrorist financing risks more effectively and closer to real time.[19]

15. It is also important to recall that the Security Council demanded 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 present resolution, comply with their obligations under international law, including international humanitarian law, international human rights law and international refugee law".[20] The Council further urged 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".[21] When designing and implementing measures to counter the financing of terrorism, Member States should also take into account unintended consequences and impacts

[17] Financial Action Task Force, "Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers". In the report, the Financial Action Task Force finds that, while some jurisdictions have made progress in putting AML/CFT regulations in place, global implementation is still lagging. Several Governments have yet to take any significant steps to regulate the sector, and these countries need to prioritize implementing the Financial Action Task Force standards in full as a matter of urgency. Based on 130 mutual evaluation and follow-up reports issued since the revised recommendation 15 was adopted in 2019, 75 per cent of jurisdictions are only partially or not compliant with the Financial Action Task Force requirements, which is identical to the figure in April 2023 (75 per cent partially compliant or non-compliant jurisdictions, or 73 of 98) and shows negligible improvement. See also Financial Action Task Force, "Status of implementation of recommendation 15 by FATF members and jurisdictions with materially important VASP activity", March 2024, available at https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf.coredownload.pdf; Counter-Terrorism Committee Executive Directorate, "Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions", December 2022, pp. 16–18, available at www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_2022_cft_gaps_assessment_final.pdf.

[18] See also Financial Stability Board, "G20 roadmap for enhancing cross-border payments: priority actions for achieving the G20 targets", 23 February 2023, available at https://www.fsb.org/2023/02/g20-roadmap-for-enhancing-cross-border-payments-priority-actions-for-achieving-the-g20-targets/.

[19] See for example Financial Action Task Force, *Opportunities and Challenges of New Technologies for AML/CFT*.

[20] Resolution 2462 (2019), para. 6; see also resolution 2617 (2021), in which the Security Council recalled the importance of fully respecting the rights to freedom of expression and association of individuals in civil society and freedom of religion or belief and underlined the importance of adopting effective and proportionate CFT measures relevant to non-profit organizations.

[21] Resolution 2462 (2019), para. 24; see also resolution 2482 (2019), para. 16, which extended this requirement to all measures taken to counter terrorism. Furthermore, certain financial transactions as defined in paragraph 1 of resolution 2664 (2022) necessary to ensure the timely delivery of humanitarian assistance and other activities that support basic human needs are permitted in situations where the Security Council's targeted financial sanctions are applicable, and are not a violation of the relevant asset freezes (see also resolution 2761 (2024)).

on humanitarian activity and human rights, and on legitimate activities of non-profit organizations and civil society.

16. Considering the speed at which new and emerging financial technologies are advancing, allowing for real-time cross-border movement of funds, before the global regulatory system has applied controls and reporting requirements to the entities involved, Member States should develop measures to identify, assess and counter the associated threats. There is a need to increase the exchange of information and practices in this area by relevant authorities, civil society, academia and the private sector; enhance international cooperation and mutual legal assistance; strengthen the understanding of the emerging risks; analyse the opportunities offered and risks posed by modern financial technologies in the context of counter-terrorism; and explore ways to achieve a more holistic global approach.

Non-binding guiding principle 1: enhance the understanding of the terrorist financing risks associated with new and emerging financial technologies and fundraising methods

17. Understanding the nature and scope of the threat remains the first and critical step for developing appropriate responses, particularly given the potential benefits of these technologies to counter terrorism and its financing. The ways in which new technologies are abused by terrorist actors can vary considerably depending on the proximity and scope of the terrorism activity, availability of technologies, the terrorists' financial needs, and the regional and economic contexts. Overfocusing on risks related to certain types of new products or services, while overlooking more traditional and commonly used ones for terrorism financing purposes,[22] is not consistent with the risk-based approach. Therefore, risk understanding should be based on assessing terrorists' financial tradecraft in context-specific circumstances to ascertain how, when and why terrorists adopt new and emerging technologies to finance their activities. Responses that are based on assumed, rather than evidence-based, risks of terrorist financing are often unnecessary and disproportionate to the advantages of new financial technologies, including their potential to address financial exclusion, and risk violating international law, including international human rights law.

18. In their efforts to analyse threats, risks and vulnerabilities associated with the use of new and emerging financial technologies for terrorist financing purposes, Member States should consider:

(a) Conducting regular, inclusive and evidence-based terrorist financing national risk assessments that take into account each State's unique operating climate and context as well as global and regional terrorist financing trends. To stay up to date, comprehensive risk assessments should be conducted at periodic intervals (and complemented by sectoral risk assessments, as applicable);

(b) Integrating into their national risk assessments analysis of terrorist financing risks associated with new and emerging payment technologies and fundraising methods and identify vulnerabilities of specific products and services, in a manner consistent with resolution 2462 (2019) and the relevant Financial Action Task Force recommendations;

[22] Terrorists continue to raise funds through a variety of means, including the abuse of legitimate commercial enterprise, exploitation of natural resources, abuse of non-profit organizations, donations, and proceeds of criminal activity, such as kidnapping for ransom, extortion, and trafficking in persons, cultural property, drugs and weapons. The terrorist financing-related funds continue to be moved through formal financial institutions, informal systems and cash couriers.

(c) Extending research and analysis of relevant terrorist financing threats to the widest possible variety of terrorist groups, including those motivated by xenophobia, racism and other forms of intolerance, or in the name of religion or belief, and keep abreast of regional and global trends,[23] seeking also to identify the financing methods and tools used by individual groups;

(d) Proactively working with international counterparts in jurisdictions where known terrorist financing ties have been identified;

(e) Utilizing a multi-stakeholder approach, including effective interaction and exchanges between the relevant national authorities, the private sector, civil society and academia, to develop a comprehensive picture of the existing and evolving terrorist financing risks informed by a diversity of experiences and perspectives and better understanding both the benefits of these technologies and the scale of the threat and impact on different categories of sectors and populations, including local communities, as well as region-specific realities, thus enabling the development of a tailored and proportionate response;

(f) Carrying out evidence-based assessments of terrorist financing risks associated with social media. This includes identification of specific features used for integration with payment services;[24]

(g) Consulting up-to-date methodologies issued by relevant multilateral organizations on conducting regular, inclusive and evidence-based national risk assessments for terrorist financing and, if required, requesting technical assistance in conducting such assessments;

(h) Sensitizing all relevant sectors and stakeholders to the identified benefits, risks and vulnerabilities;

(i) Taking steps to ensure that financial institutions conduct their own risk assessments prior to the launch of new products, business practices or the use of new or developing technologies, and taking appropriate measures to manage and mitigate those risks, as outlined in Financial Action Task Force recommendation 15.

Non-binding guiding principle 2: develop and implement risk-based, proportionate regulation, monitoring and supervision to prevent the abuse of new technologies for terrorist financing purposes

19. As noted during the consultations for the preparation of these non-binding guiding principles, States should continuously review and readapt, where needed, their existing regulatory frameworks to ensure that they are relevant, targeted and effective to address vulnerabilities that come with emerging financial technologies. To do this successfully, States' response measures should be built for purpose, rooted in evidence-based risk assessment rather than assumed vulnerabilities, and be in line with the risk-based approach under the Financial Action Task Force standards. They should also be balanced against the potential of new financial technologies to enhance financial inclusion as a key enabler of various Sustainable Development Goals, as well as for innovating payments and the means to transact them safely in crisis situations. As noted by the Financial Action Task Force, "innovative fintech and other financial products can support [non-profit organization] activities, especially the delivery of aid to hard-to-reach areas" and contribute to greater traceability of financial transactions, "thereby not only reducing the risk of diversion of funds, but

[23] See also S/2021/972, annex, para. 668.

[24] See also Asia/Pacific Group on Money Laundering and Middle East and North Africa Financial Action Task Force, "Social media and terrorism financing", January 2019, available at www.apgml.org/includes/handlers/get-document.ashx?d=2446bd89-b2cc-4c3c-b378-5f03658dc906.

also supporting a secure audit trail for aid delivery".[25] Conversely, disproportionally restrictive regulation and supervision of digital payment platforms can unnecessarily limit human rights and hamper the delivery of humanitarian assistance carried out by impartial humanitarian actors in a manner consistent with international humanitarian law to those in greatest need, especially in conflict- or terrorism-affected areas that lack banking or otherwise regulated financial services. Without adequate checks and balances, including monitoring and oversight, overregulation of digital payment services may place onerous burdens on humanitarian work and legitimate economic or non-profit organization activities.[26] The Security Council, in its resolution 2462 (2019), noted with grave concern the abuse of non-profit organizations by terrorists to raise, move and transfer funds; called upon Member States to implement a risk-based approach and to work cooperatively with the non-profit sector in order to prevent abuse of such organizations, including front organizations by and for terrorists; and recalled the relevant recommendations and existing guidance documents of the Financial Action Task Force in that regard, in particular its recommendation 8. The Financial Action Task Force has also noted that the interest to minimize the negative impact on legitimate beneficiaries of non-profit organization activity cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by non-profit organizations.[27] The primary objective of Financial Action Task Force recommendation 8 is to ensure that non-profit organizations are not abused by terrorists.

20. In their efforts to adequately regulate, monitor and supervise providers of new and emerging payment services, Member States should consider:

(a) Developing risk-based regulatory and supervisory systems for relevant sectors, including virtual asset service providers, in line with related Security Council resolutions and Financial Action Task Force standards, and in full compliance with international law;

(b) Reviewing existing frameworks with all relevant stakeholders in an ongoing manner so they remain adequate to address new and evolving risks and extending such frameworks to new and emerging service providers, as applicable, identifying gaps and potential for duplication or overregulation;

(c) Strengthening frameworks that allow for inter-agency cooperation with a view to intensifying the timely exchange of financial intelligence, domestically and internationally,[28] consistent with applicable Financial Action Task Force recommendations;

(d) Ensuring that national risk-based AML/CFT frameworks apply to virtual asset service providers in line with the Financial Action Task Force standards to ensure the traceability of transactions, including through the implementation of the so-called "Financial Action Task Force travel rule" that requires virtual asset service providers and other financial institutions to share relevant originator and beneficiary information alongside certain virtual asset transactions;

[25] Financial Action Task Force, *Best Practices: Combating the Terrorist Financing Abuse of Non-Profit Organizations* (Paris, 2023), para. 129, available at https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP-Combating-TF-Abuse-NPO-R8.pdf.coredownload.inline.pdf.

[26] In this regard and with reference to resolution 2462 (2019), the Financial Action Task Force also recognizes the importance of ensuring that the implementation of its recommendations, in particular recommendation 8, the objective of which is to ensure that non-profit organizations are not abused by terrorists and terrorist organizations, does not adversely and disproportionately affect non-profit organizations, and furthermore, does not unduly hinder civil society and the delivery of humanitarian assistance (ibid., para. 113).

[27] Financial Action Task Force, interpretive note to recommendation 8, para. 5 (d).

[28] See also resolution 2462 (2019); and S/2021/972, annex, para. 673.

(e) Developing appropriate and effective national frameworks and mechanisms to detect unregistered providers operating new and emerging financial services and transacting funds using new technologies;

(f) Improving the effectiveness of monitoring compliance of registered financial service providers operating new and emerging technologies (including mobile money operators) by developing effective compliance oversight programmes, including through the enforcement of robust onboarding and customer due diligence procedures;

(g) Testing market innovations to ensure that they meet the needs of target audiences while upholding regulatory standards (e.g. so-called "regulatory sandboxes" that allow a product to conditionally operate under a no-objection granted by the regulator). When set up in tandem, such mechanisms could allow the private sector and regulators to collaboratively identify risks, build mutual understanding and pilot a regulatory framework;

(h) Developing frameworks to monitor, detect and disrupt abuse of social media platforms for terrorist financing purposes, while ensuring full compliance with applicable international law;

(i) Implementing outreach to and awareness-raising initiatives in an ongoing manner for relevant service providers and other potentially vulnerable stakeholders that are not subject to AML/CFT reporting obligations, including social media and certain crowdfunding platforms, to alert them to terrorist financing risks, typologies and red flags, as well as to the regulations in place and tools available to mitigate and/or report suspicious activity;

(j) Utilizing a multi-stakeholder approach with the meaningful participation of, inter alia, the private sector, civil society and the public, when designing terrorist financing risk mitigation measures.

Non-binding guiding principle 3: effectively detect and disrupt the abuse of new technologies for the purposes of terrorist financing

21. States should avoid politicization of issues of international counter-terrorism cooperation, including in AML/CFT, and continue to enhance their capacity to effectively detect and disrupt the abuse of new technologies for the purposes of terrorist financing, including through investigation and prosecution, reinforced inter-agency and international cooperation, establishing and utilizing relevant mechanisms to provide mutual legal assistance, and developing public-private partnerships. As noted by the Financial Action Task Force,[29] terrorist financing disruption strategies encompass a broad range of tools and practices, implemented by numerous counter-terrorism/CFT authorities, operating in coordination with one another and sharing information in a timely manner. In this regard, national coordinating committees play a fundamental role in the development and implementation of effective terrorist financing disruption strategies. A national counter-terrorism/CFT strategy based on a thorough and up-to-date risk assessment provides the framework for operational cooperation between relevant agencies and between relevant agencies and the private sector, including with respect to new and evolving financial technologies. As such, terrorist financing disruption strategies go beyond reactive investigative actions and are aimed at using the full and cross-disciplinary spectrum of legal, administrative and policy measures to disrupt and degrade the capacity of terrorist groups to operate. The range of targeted disruption actions could include targeted financial sanctions; non-public advisories and alerts;

[29] Financial Action Task Force, "Terrorist financing disruption strategies", October 2018 (non-public).

the physical disruption of cash movement and storage; criminal sanctions against terrorists, facilitators and financiers; and non-conviction-based forfeiture against terrorist-related entities. The peculiarities of each financing method, and the actors involved, will then dictate the appropriate response.

22. In their efforts to effectively detect and disrupt the abuse of new technologies for the purposes of terrorist financing, Member States should consider:

(a) Developing multi-agency and, where applicable, multi-stakeholder coordination mechanisms that include relevant policymakers, judiciary and law enforcement authorities, financial investigation units, supervisory authorities and regulators to exchange information and intelligence;[30]

(b) Establishing frameworks and procedures for feedback mechanisms between law enforcement, financial intelligence units and reporting entities from relevant sectors to improve the quality of reports and financial intelligence products, as well as to support trend monitoring and strategic analysis;

(c) Developing and enhancing, in an ongoing manner, the capacity of relevant national authorities to follow the money more effectively, including through parallel financial investigations in terrorism cases, with the use of new analytical methods, tools and technologies, as well as the requisite independent oversight and review mechanisms. It is essential to continue to invest in technologies and training and mobilize top experts as well as to invest in privacy-enhancing technology to protect sensitive information;

(d) Making optimal use of new and emerging financial and regulatory technologies to contribute to the effective implementation of AML/CFT measures.[31] Technology should be used responsibly to facilitate data collection, processing and analysis and help to identify and manage terrorist financing risks more effectively and closer to real time;

(e) Including appropriate safeguards and features for new AML/CFT solutions, including accountability and transparency of processes and outcomes, oversight by humans, respect for privacy and data protection,[32] and alignment with global technical standards and best practices;

(f) Developing and implementing policies and procedures for law enforcement and other competent authorities to investigate the use of the Internet and social media for terrorist finance[33] and to obtain access to evidence in a timely manner, in full compliance with applicable international law. Increasing social media investigative capabilities in relation to terrorist financing is important, as is developing special operating procedures for engaging with operators and service providers in other jurisdictions;[34]

---

[30] See also resolution 2462 (2019), para. 19.

[31] See Financial Action Task Force, *Opportunities and Challenges of New Technologies for AML/CFT*.

[32] See also Financial Action Task Force recommendation 2, which highlights that information exchange should include cooperation and coordination between relevant authorities "to ensure the compatibility of [CFT] requirements with data protection and privacy rules and other similar provisions (e.g. data security/localization)".

[33] See also Asia/Pacific Group on Money Laundering and Middle East and North Africa Financial Action Task Force, "Social media and terrorism financing".

[34] See also Tom Keatinge and Florence Keen, "Social media and terrorist financing: what are the vulnerabilities and how could public and private sectors collaborate better?", Global Research Network on Terrorism and Technology: Paper No. 10 (Royal United Services Institute for Defence and Security Studies, 2019), available at https://static.rusi.org/20190802_grntt_paper_10.pdf.

(g) Ensuring that mechanisms in place to implement terrorist assets freezing requirements without delay effectively extend to assets transacted through new and emerging financial technologies, including virtual assets, with due process and procedural safeguards in place;

(h) Including wallet addresses directly associated with individuals or entities designated as terrorist in the identifying information communicated to the private sector;

(i) Given the cross-border nature of the threat, promptly sharing early warning type information and, where appropriate, financial intelligence between States,[35] including with regard to suspicious virtual asset service provider activity;

(j) Making full use of international and regional information exchange and cooperation tools, including relevant International Criminal Police Organization databases and analytical files, and sharing acquired expertise and knowledge for the use of other Member States;

(k) Enhancing collaboration with the Counter-Terrorism Committee Executive Directorate, the Financial Action Task Force, Financial Action Task Force-style regional bodies and other relevant international and regional organizations to explore further ways to strengthen the effectiveness of the international response to the use of new payment and fundraising methods for terrorist purposes and establish regular sharing of effective practices in this field;

(l) Developing robust public-private partnerships to share information, enhance understanding of evolving trends, increase the knowledge and skills of relevant experts and stakeholders, including gatekeepers, and help to strengthen the integrity of the financial sector.[36] Such partnerships should include dialogue between financial intelligence units and the relevant financial technology sector with regard to data-sharing as part of suspicious activity reporting,[37] with a clear legal basis for the sharing of information, including criteria and purposes for which information may be shared and the entities with which it can be shared. With regard to social media, such public-private partnerships help to ensure that the CFT efforts of social media companies are informed and effective.[38] Public-private partnerships have also served as a useful forum for the authorities to disseminate regular guidance to the private sector, including risk indicators;

(m) Building upon effective public-private partnerships to use the available technology and data, including blockchain intelligence, to enhance operational and tactical analysis, map terrorist financial networks, and track and report suspicious activity.

Non-binding guiding principle 4: evaluate the impact of measures to counter the financing of terrorism in relation to new and emerging technologies

23. Regulators are placed in the challenging position of balancing the need to encourage new payment technologies for the public benefit while also ensuring an

[35] See also resolution 2462 (2019), para. 28 (a).

[36] See also ibid., para. 22. During the technical sessions led by the Counter-Terrorism Committee Executive Directorate, the experience of the Terrorist Financing Task Force of the Financial Expertise Centre in the Kingdom of the Netherlands was cited as a good practice for cooperation and information-sharing between the public and private sectors. As a general trend, those States that have created active public-private partnerships report an increase in the quality and quantity of suspicious transaction reports received in relation to terrorist financing. See also S/2020/493, para. 68; and S/2021/972, annex, para. 677.

[37] See also Stephen Reimer and Matthew Redhead, *Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks, RUSI Occasional Paper* (Royal United Services Institute for Defence and Security Studies, 2022).

[38] See also Keatinge and Keen, “Social media and terrorist financing”.

effective regulatory system that protects against criminal and terrorist misuse. As noted above, technology has the ability to improve the traceability of financial transactions and streamline due diligence in banking and can therefore reduce burdens and delays in the work of non-profit organizations and humanitarian actors. At the same time, and as underscored by the Financial Action Task Force, there is a need to "ensur[e] these technological solutions are not discriminatory in nature, or used in a discriminatory manner".[39]

24. In their efforts to evaluate impact and any unintended consequences of new CFT measures related to new technologies on human rights, financial inclusion, legitimate non-profit organization activities as well as on exclusively humanitarian activity carried out by impartial humanitarian actors in a manner consistent with international humanitarian law,[40] and to effectively mitigate those consequences, States should consider:

(a) Introducing clear, transparent, international human rights law-compliant and gender-sensitive policies to guide the use of new technologies and ensure careful consideration of the potential risks and consequences;

(b) Utilizing a multi-stakeholder approach when reviewing and proactively managing any potential and actual adverse impact of CFT measures related to new technologies on human rights, developing guidelines, review tools and benchmarks for such impact assessments and designing mitigation measures, to include the relevant national authorities, the private sector, civil society and academia. In addition, standing dedicated mechanisms, platforms or channels can help civil society and other relevant stakeholders to effectively communicate any unintended adverse consequences of the newly developed CFT measures on the exercise of their rights and their legitimate activities and, where applicable, to seek judicial review;

(c) When designing data systems and processes that facilitate access, retrieval and analysis of relevant information (including through the use of machine learning and automating financial crime risk detection), ensuring that data-sharing frameworks and protocols are in place to facilitate information exchange between different entities involved in CFT, in line with international human rights law;

(d) When evaluating effectiveness, adopting a data-driven and inclusive approach to ensure meaningful insights. By regularly reviewing and analysing relevant data, policymakers and stakeholders can identify areas for improvement, refine strategies and enhance the overall effectiveness of CFT efforts;

(e) As financial technologies continue to evolve and their use in AML/CFT is increasing, strengthening independent oversight and accountability mechanisms for relevant measures in accordance with the due process and procedural safeguards. Oversight mechanisms should also ensure that relevant public-private partnerships adhere to data protection or privacy obligations under national legislation as well as applicable international law;

(f) Ensuring that the measures designed to address identified terrorist financing risks related to new payment technologies do not unduly disrupt or negatively affect legitimate non-profit organization activity. States should consider whether the focused, proportionate and risk-based measures already in place in relation to the Financial Action Task Force-defined subset of non-profit

[39] Financial Action Task Force, *Best Practices: Combating the Terrorist Financing Abuse of Non-Profit Organizations*, para. 129. The Financial Action Task Force notes in particular that "human oversight may be necessary when using algorithms to avoid perpetuating existing biases (religious, ethnic, gender and others)".

[40] See also resolution 2462 (2019), fifth preambular paragraph and paras. 23 and 24.

organizations,[41] including self-regulatory and internal risk mitigation measures, can also be used to address the new risks and vulnerabilities;

(g) Establishing standing mechanisms, platforms or channels allowing civil society and other relevant stakeholders to communicate any unintended adverse consequences of the newly developed CFT measures on the exercise of their rights and their legitimate activities and, where applicable, to seek judicial review. Outreach should include meaningful and collaborative dialogue between government, the private sector and civil society, including on unforeseen challenges and consequences;

(h) Ensuring that new regulations designed to enhance the traceability and transparency of financial transactions do not breach the right to be free from unlawful or arbitrary interference with privacy and other human rights, or result in the surveilling of humanitarian aid beneficiaries, but rather reinforce privacy protections through the lawful use of personal information;

(i) Providing guidance to the private sector on the elimination of bias and faulty data in detection models, including through human feedback loops, and the most effective way to share data with the authorities in accordance with applicable international human rights law;

(j) Conducting further research and developing minimum standard-setting for the effectiveness of financial technology and its impact on different stakeholder groups;

(k) Documenting international human rights law-compliant and gender-sensitive good practices and lessons learned on the design, development, assessment and evaluation of AML/CFT technologies, with input from the private sector and civil society.

[41] For the purposes of Financial Action Task Force recommendation 8, “non-profit organization” refers to a legal person or arrangement or organization 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”. This recommendation was revised in 2016 to clarify the subset of non-profit organizations which should be made subject to supervision and monitoring. As further revised in November 2023, recommendation 8 and its interpretive note call for “focused, proportionate and risk-based measures, without unduly disrupting or discouraging legitimate [non-profit organization] activities” to protect the non-profit organization sector from terrorist financing. According to the interpretive note to Financial Action Task Force recommendation 8 (para. 6):

“NPOs [non-profit organizations] are at varying degrees of risk of TF [terrorist financing] abuse by virtue of their types, activities or characteristics and the majority may represent low risk. Without prejudice to the requirements of recommendation 1:

“(a) Countries should identify organizations which fall within the FATF definition of NPOs.

“(b) Countries should conduct a risk assessment of these NPOs to identify the nature of TF risks posed to them.”